STORMWATCH

CYBERSECURITY NEWS

Dateline: 2024-03-26

LIKE

SUBSCRIBE

Storm ⚡ Watch by GreyNoise Intelligence

GreyNoise Intelligence

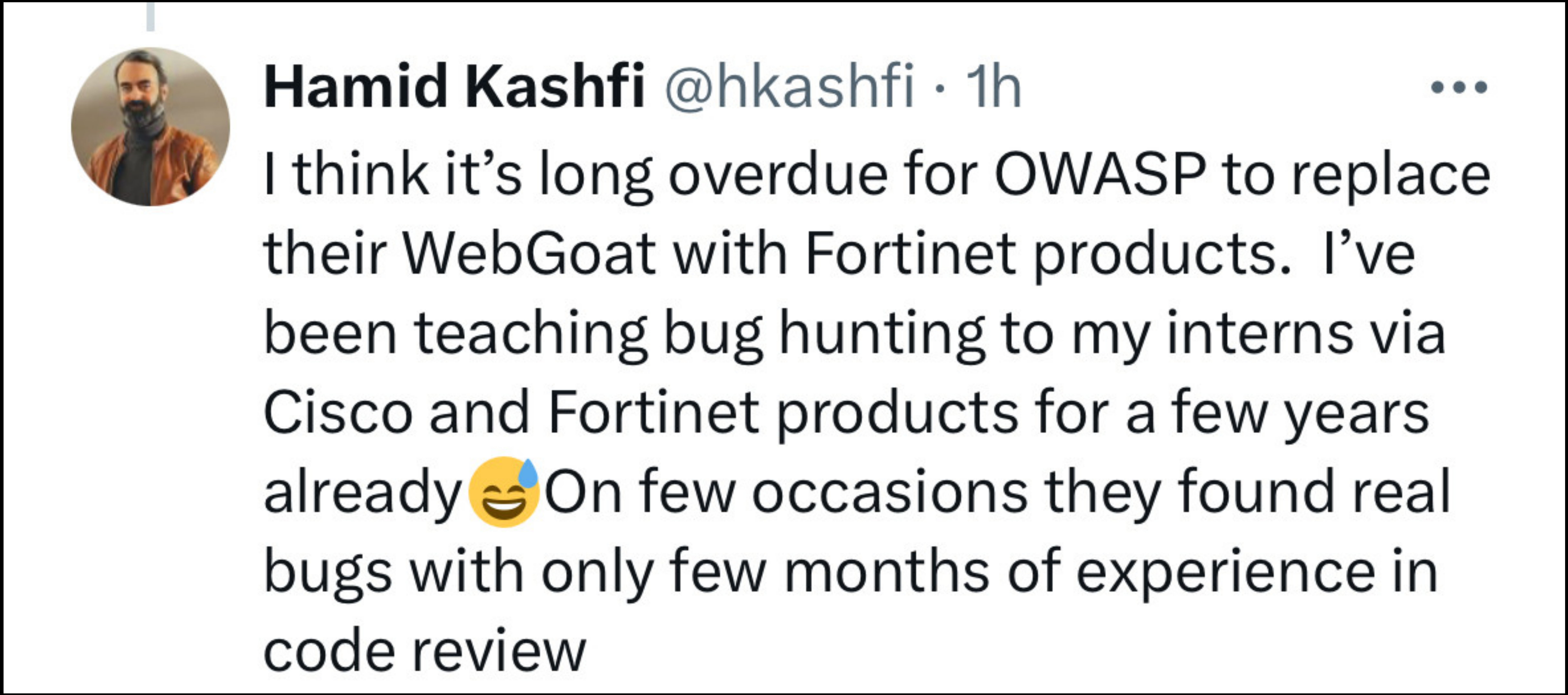
TECHNOLOGY · UPDATED WEEKLY

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



Hamid Kashfi @hkashfi · 1h

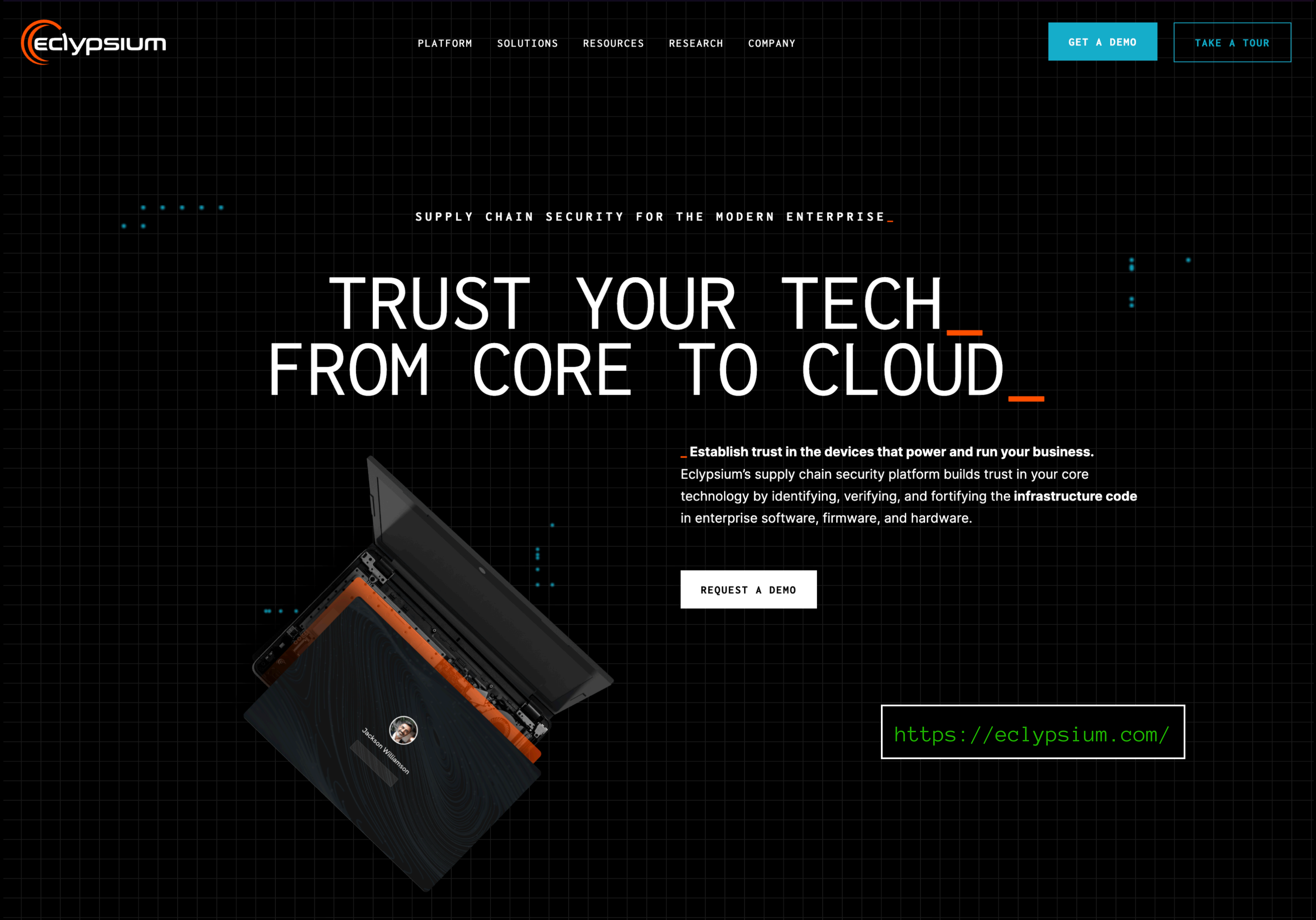
I think it’s long overdue for OWASP to replace their WebGoat with Fortinet products. I’ve been teaching bug hunting to my interns via Cisco and Fortinet products for a few years already😅On few occasions they found real bugs with only few months of experience in code review

STORM ⚡ WATCH

CYBERSECURITY NEWS

CYBERSIDE CHAT

👻 🔥



SUPPLY CHAIN SECURITY FOR THE MODERN ENTERPRISE_

TRUST YOUR TECH_ FROM CORE TO CLOUD_

_ **Establish trust in the devices that power and run your business.** Eclypsium's supply chain security platform builds trust in your core technology by identifying, verifying, and fortifying the **infrastructure code** in enterprise software, firmware, and hardware.

https://eclypsium.com/

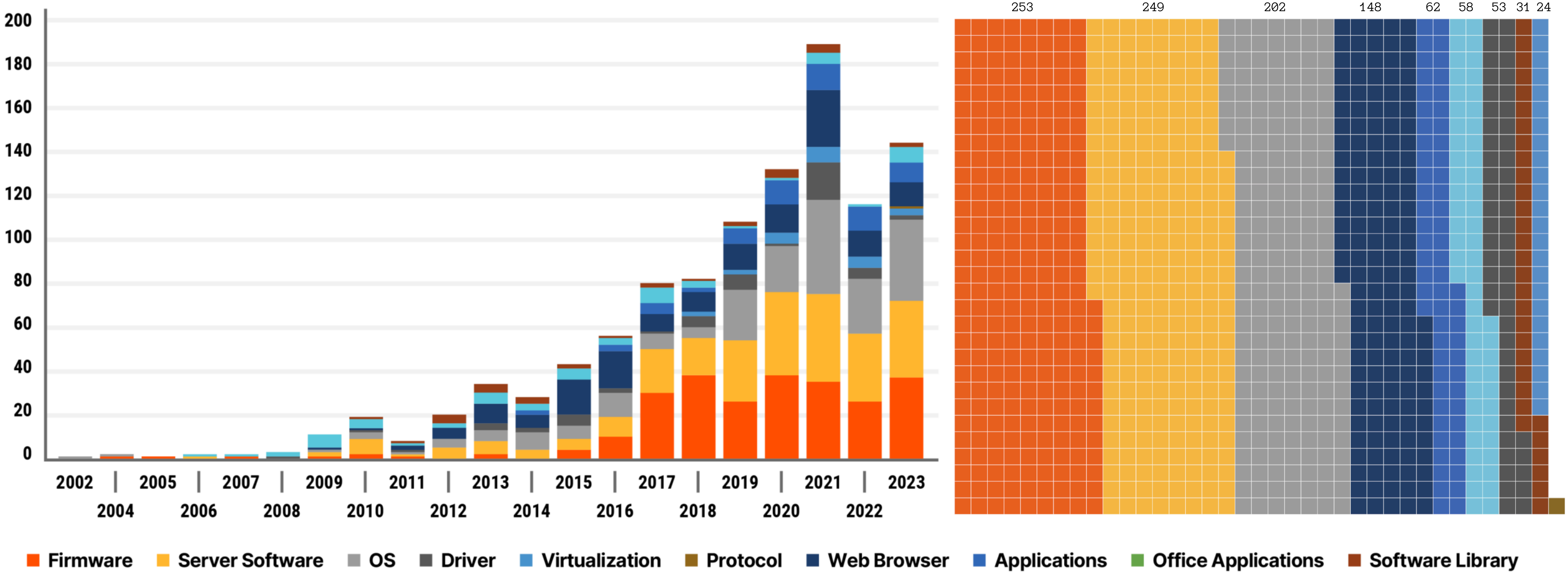
https://eclypsium.com/research/attack-of-the-supply-chain/

SUPPLY CHAIN WARS

Episode X

ATTACK OF THE SUPPLY CHAIN

Like many in our field, I am a Star Wars nerd. I could quickly fill this post with several thoughts and



https://eclypsium.com/blog/analyzing-cisa-kev-data-to-understand-danger/

STORMWATCH

CYBERSECURITY NEWS

CYBER SPOTLIGHT

TECH

Sanctions on APT31 Hackers

The United States Treasury Department has imposed sanctions on individuals and entities linked to the Chinese state-sponsored hacking group known as APT31. This group has been implicated in a series of cyberattacks targeting U.S. critical infrastructure sectors, including defense, aerospace, and energy. The sanctions specifically target a front company for the Ministry of State Security (MSS), and two Chinese nationals, for their roles in these campaigns. The sanctions are part of a collaborative effort with the U.S. Department of Justice, Federal Bureau of Investigation (FBI), Department of State, and the United Kingdom Foreign, Commonwealth & Development Office (FCDO).

Homework

- https://home.treasury.gov/news/press-releases/jy2205
- https://www.securityweek.com/us-treasury-slaps-sanctions-on-china-linked-apt31-hackers/
- https://www.theguardian.com/technology/2024/mar/25/us-sanctions-chinese-hackers
- https://therecord.media/us-sanctions-chinese-hackers-infrastructure-attacks
- https://www.reuters.com/technology/cybersecurity
- https://nymag.com/intelligencer/article/big-tech-still-has-a-big-addiction-to-china.html
- https://www.aljazeera.com/news/2024/3/25/
- https://www.voanews.com/a/us-uk-bring-charges-sanctions-in-response-to-chinese-hacking-operation/7542641.html

Volt Typhoon & H2O Facilities

Volt Typhoon is another Chinese state-sponsored hacking group that has been compromising U.S. critical infrastructure, including water and wastewater systems. The White House, in collaboration with the Environmental Protection Agency (EPA), announced the formation of a Water Sector Cybersecurity Task Force in response to these threats. The task force aims to engage state water sectors and water government coordinating councils to reduce the risks of cyberattacks on nationwide water systems. This initiative follows the discovery that Volt Typhoon has compromised the IT environments of multiple U.S. critical infrastructure organizations with the end goal of a future cyberattack.

Homework

- https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a
- https://www.meritalk.com/articles/
- https://www.darkreading.com/ics-ot-security/new-us-warning-highlights-vulnerability-of-us-water-systems-to-cyberattacks

China Hacks U.K. Politihacks

The U.K. has also been a target of Chinese state-sponsored cyber espionage. Hackers affiliated with APT31 have been accused of conducting a years-long cyber-attack targeting politicians, journalists, and businesses. The operation saw political dissidents and critics of China targeted by sophisticated phishing campaigns, resulting in some email systems and networks being compromised. The U.K. government announced sanctions against individuals and a front company linked to APT31. The New Zealand government has also raised concerns with the Chinese government about its involvement in an attack.

Homework

- https://www.theguardian.com/politics/live/2024/mar/25/rishi-sunak-conservatives-oliver-dowden-china-cyber-attacks-keir-starmer-labour-wales-uk-politics-live

China Expands State Secrets / "Work Secrets" Law

China has revised its state secrets law, which now requires business entities in China to identify and disclose "work secrets," or non-classified information, to the government. This revision is purposely ambiguous, allowing China to potentially force U.S. tech firms to turn over proprietary information that could be used to target the U.S. government or impact the data security of Americans. The law poses a significant dilemma for U.S. tech companies operating in China, as compliance could threaten U.S. national security, while refusal could result in losing access to the Chinese market.

Homework

- https://thehill.com/opinion/technology/
- https://www.forbes.com/sites/lorenthompson/2023/12/14/why-chinas-growing-challenge-to-big-tech-is-a-problem-for-the-pentagon/?sh=58d510604990
- https://www.cnbc.com/2024/02/28/china-doubles-down-on-national-security-expanding-its-state-secrets-law.html
- http://politics.people.com.cn/n1/2024/0227/c1001-40184585.html

U.S. vs. TikTok

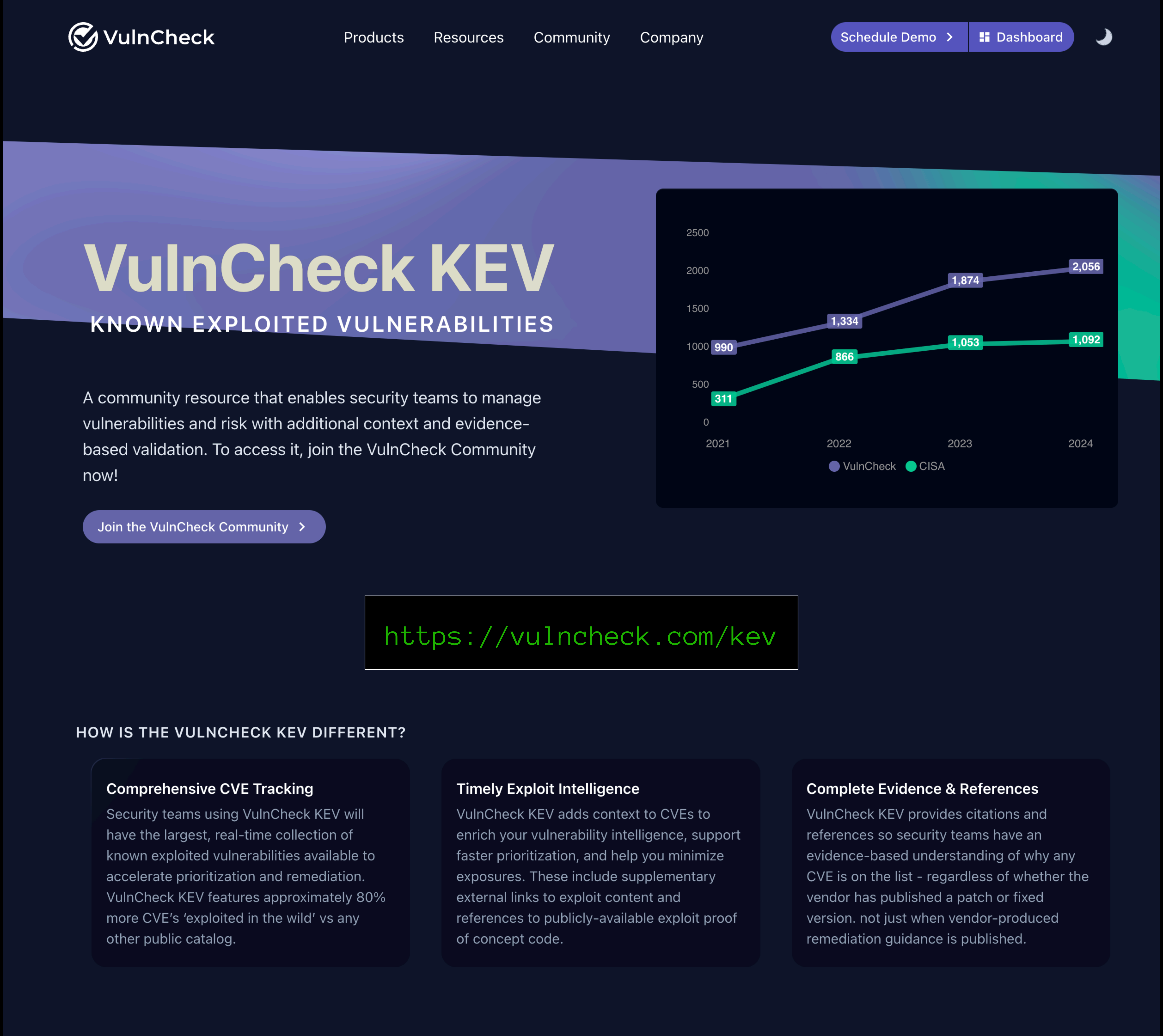
The U.S. government's scrutiny of TikTok, a popular social media platform owned by the Chinese company ByteDance, has escalated amid concerns over national security and data privacy. There have been discussions and reactions to the potential ban of TikTok in the U.S., with China criticizing the move as politicization of cybersecurity issues. The debate centers around the risks associated with the Chinese government's potential access to the data of U.S. citizens through TikTok, which has led to calls for the app to be banned or its operations in the U.S. to be segregated from its parent company.

Homework

- https://www.cnn.com/2024/03/14/tech/china-reactions-tiktok-potential-ban-intl-hnk/index.html

STORM WATCH

CYBERSECURITY NEWS



VulnCheck KEV

KNOWN EXPLOITED VULNERABILITIES

A community resource that enables security teams to manage vulnerabilities and risk with additional context and evidence-based validation. To access it, join the VulnCheck Community now!

https://vulncheck.com/kev

HOW IS THE VULNCHECK KEV DIFFERENT?

Comprehensive CVE Tracking

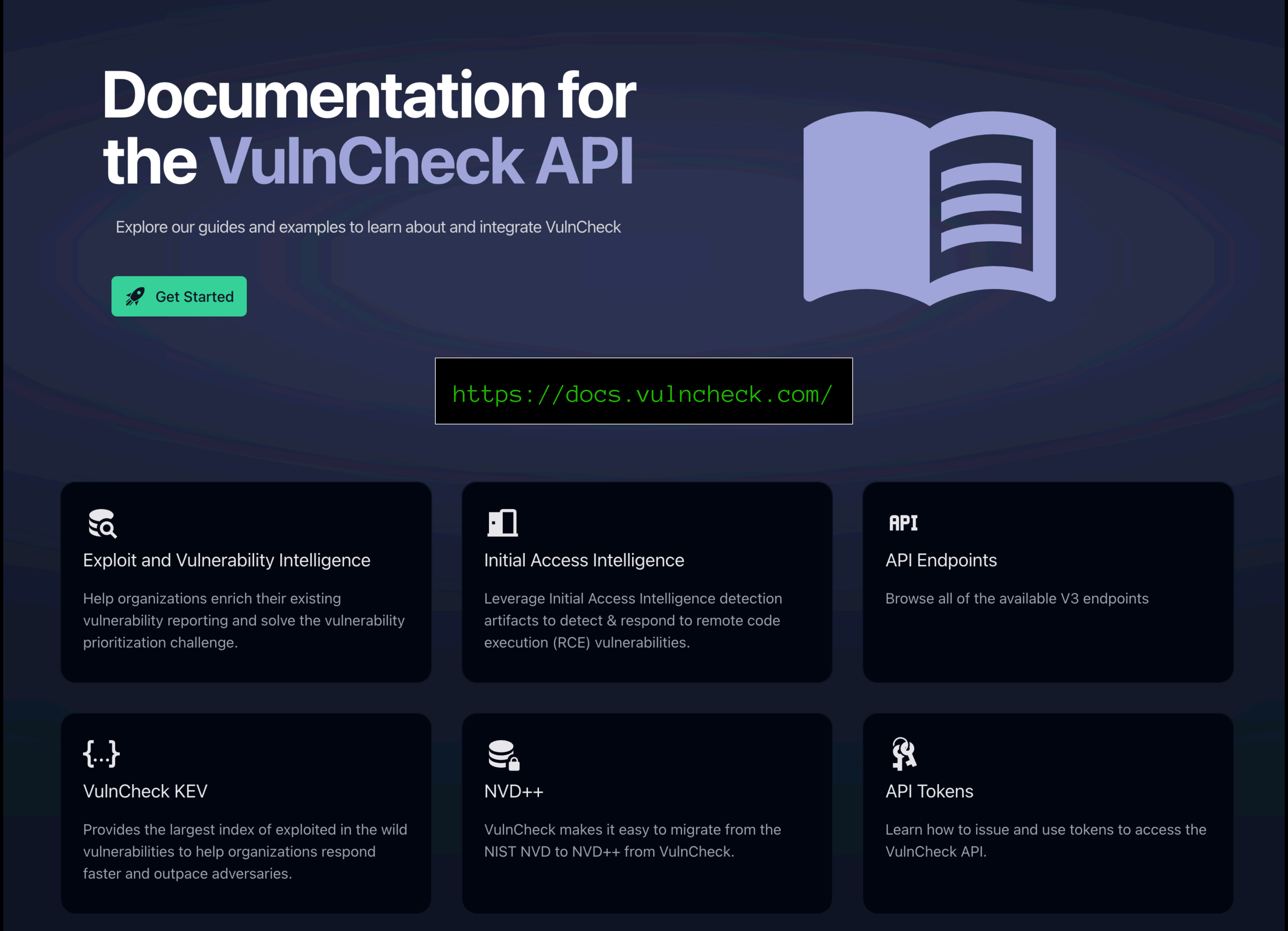
Security teams using VulnCheck KEV will have the largest, real-time collection of known exploited vulnerabilities available to accelerate prioritization and remediation. VulnCheck KEV features approximately 80% more CVE's 'exploited in the wild' vs any other public catalog.

Timely Exploit Intelligence

VulnCheck KEV adds context to CVEs to enrich your vulnerability intelligence, support faster prioritization, and help you minimize exposures. These include supplementary external links to exploit content and references to publicly-available exploit proof of concept code.

Complete Evidence & References

VulnCheck KEV provides citations and references so security teams have an evidence-based understanding of why any CVE is on the list - regardless of whether the vendor has published a patch or fixed version. not just when vendor-produced remediation guidance is published.



Documentation for the VulnCheck API

Explore our guides and examples to learn about and integrate VulnCheck

```
https://docs.vulncheck.com/
```

Exploit and Vulnerability Intelligence

Help organizations enrich their existing vulnerability reporting and solve the vulnerability prioritization challenge.

Initial Access Intelligence

Leverage Initial Access Intelligence detection artifacts to detect & respond to remote code execution (RCE) vulnerabilities.

API Endpoints

Browse all of the available V3 endpoints

VulnCheck KEV

Provides the largest index of exploited in the wild vulnerabilities to help organizations respond faster and outpace adversaries.

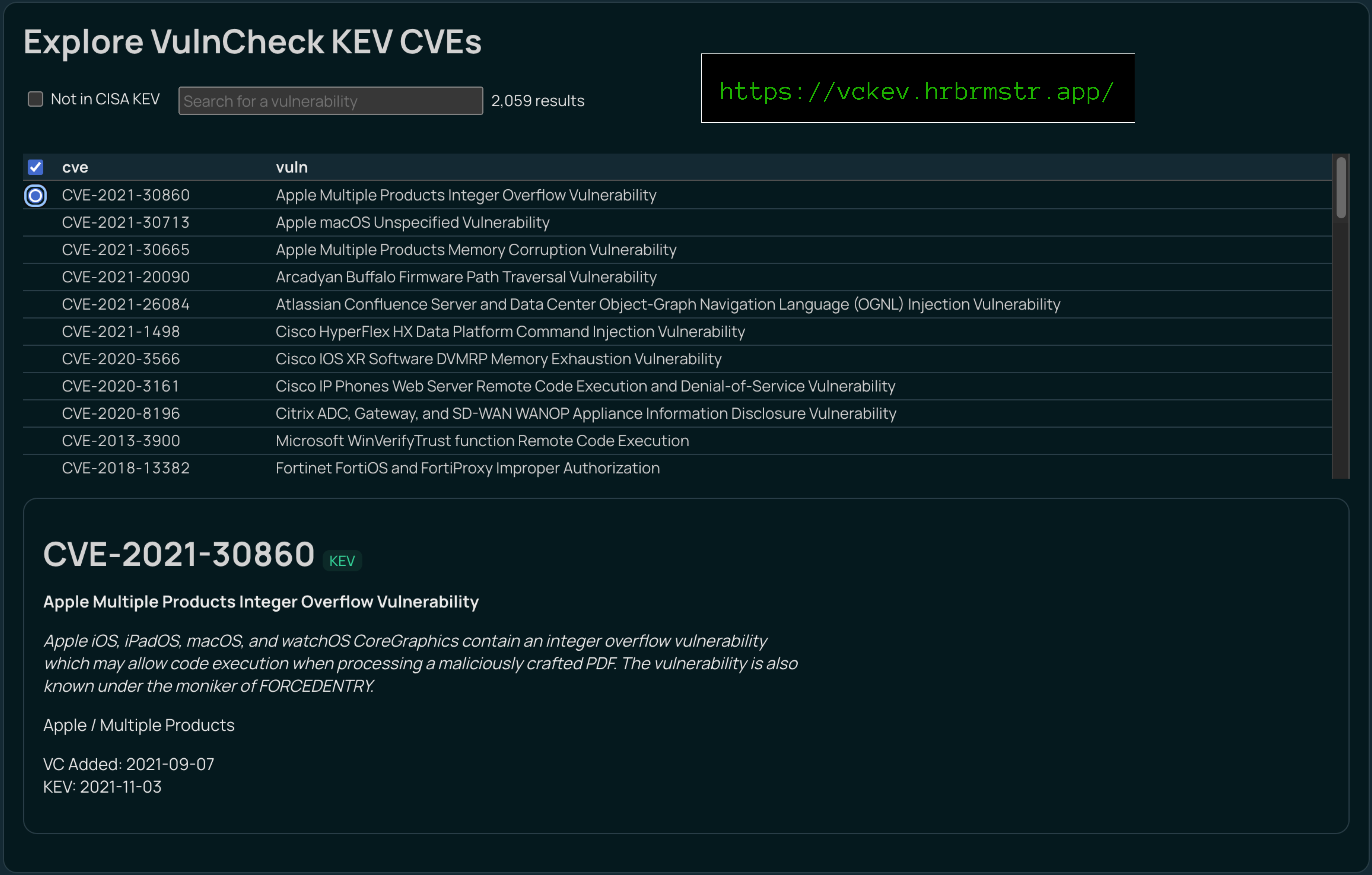
NVD++

VulnCheck makes it easy to migrate from the NIST NVD to NVD++ from VulnCheck.

API Tokens

Learn how to issue and use tokens to access the VulnCheck API.

VulnCheck KEV



Explore VulnCheck KEV CVEs

☐ Not in CISA KEV Search for a vulnerability 2,059 results

https://vckev.hrbrmstr.app/

☑	cve	vuln
●	CVE-2021-30860	Apple Multiple Products Integer Overflow Vulnerability
	CVE-2021-30713	Apple macOS Unspecified Vulnerability
	CVE-2021-30665	Apple Multiple Products Memory Corruption Vulnerability
	CVE-2021-20090	Arcadyan Buffalo Firmware Path Traversal Vulnerability
	CVE-2021-26084	Atlassian Confluence Server and Data Center Object-Graph Navigation Language (OGNL) Injection Vulnerability
	CVE-2021-1498	Cisco HyperFlex HX Data Platform Command Injection Vulnerability
	CVE-2020-3566	Cisco IOS XR Software DVMRP Memory Exhaustion Vulnerability
	CVE-2020-3161	Cisco IP Phones Web Server Remote Code Execution and Denial-of-Service Vulnerability
	CVE-2020-8196	Citrix ADC, Gateway, and SD-WAN WANOP Appliance Information Disclosure Vulnerability
	CVE-2013-3900	Microsoft WinVerifyTrust function Remote Code Execution
	CVE-2018-13382	Fortinet FortiOS and FortiProxy Improper Authorization

CVE-2021-30860 KEV

Apple Multiple Products Integer Overflow Vulnerability

Apple iOS, iPadOS, macOS, and watchOS CoreGraphics contain an integer overflow vulnerability which may allow code execution when processing a maliciously crafted PDF. The vulnerability is also known under the moniker of FORCEDENTRY.

Apple / Multiple Products

VC Added: 2021-09-07
KEV: 2021-11-03

STORMWATCH

CYBERSECURITY NEWS

SHAMELESS SELF-PROMOTION

https://info.greynoise.io/webinar/future-of-honeypots

WEBINAR

The Future of Honeypots in an Age of Targeted Attacks

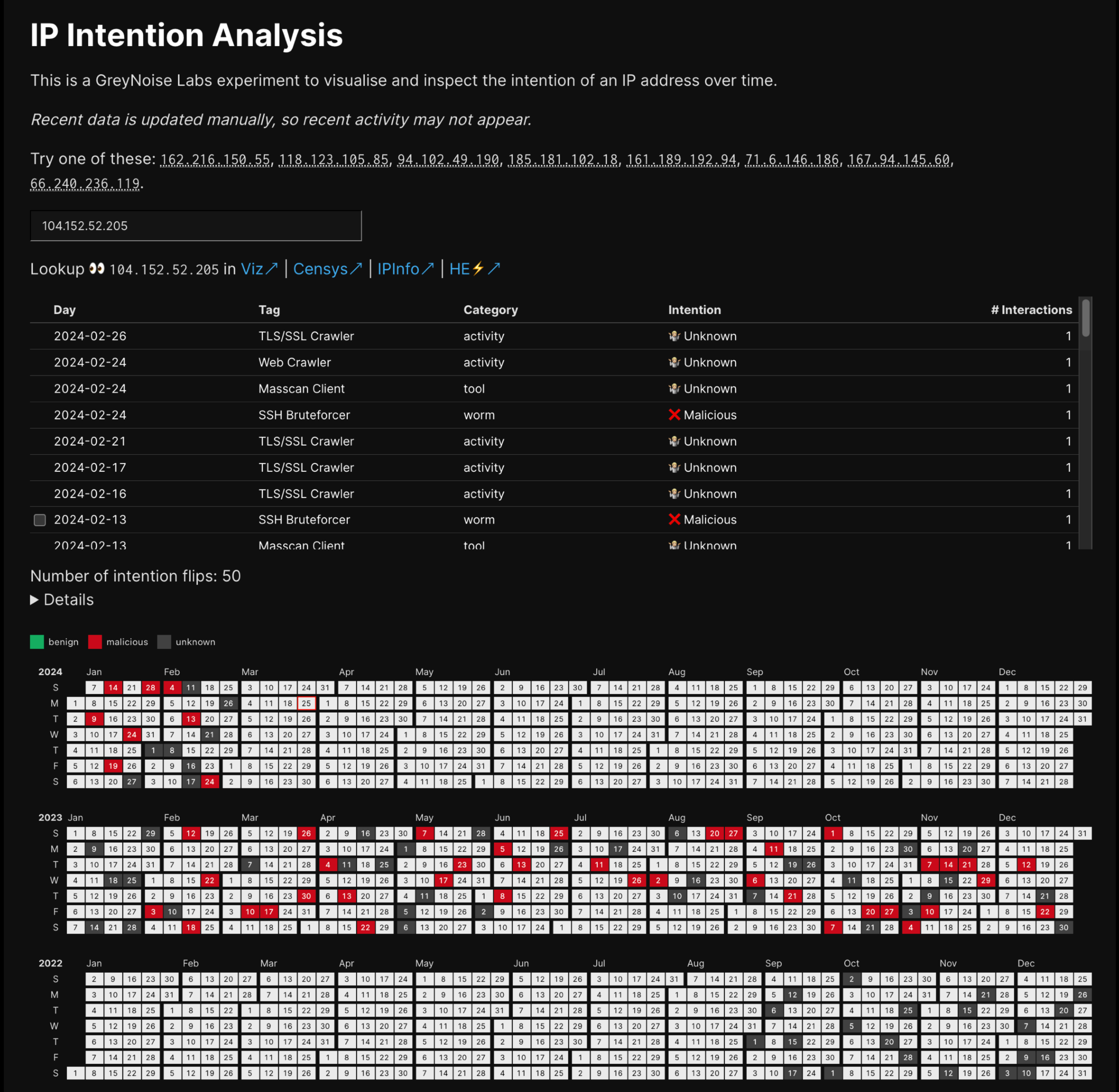
STORMWATCH

CYBERSECURITY NEWS

TAG ROUND-UP

- Well-Known Scanner
- Joomla facileforms Arbitrary File Upload Attempt
- Joomla JBcatalog Arbitrary File Upload Attempt
- Joomla JBcatalog Arbitrary File Upload Vuln Check
- Dell SonicWALL Scrutinizer methodDetail SQL Injection Attempt (CVE-2014-4977)
- Fortra FileCatalyst Workflow Web Portal Scanner
- Schuhfried Testing Platform CVE-2023-38995 Info Leak Attempt
- osCommerce 2.2 RCE Attempt
- Web.xml Access Attempt
- Joomla Com_Fabrik Arbitrary File Upload Attempt

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



IP Intention Analysis

This is a GreyNoise Labs experiment to visualise and inspect the intention of an IP address over time.

Recent data is updated manually, so recent activity may not appear.

Try one of these: `162.216.150.55`, `118.123.105.85`, `94.102.49.190`, `185.181.102.18`, `161.189.192.94`, `71.6.146.186`, `167.94.145.60`, `66.240.236.119`.

104.152.52.205

Lookup 👀 `104.152.52.205` in Viz↗ | Censys↗ | IPInfo↗ | HE⚡↗

	Day	Tag	Category	Intention	# Interactions
	2024-02-26	TLS/SSL Crawler	activity	🤷 Unknown	1
	2024-02-24	Web Crawler	activity	🤷 Unknown	1
	2024-02-24	Masscan Client	tool	🤷 Unknown	1
	2024-02-24	SSH Bruteforcer	worm	❌ Malicious	1
	2024-02-21	TLS/SSL Crawler	activity	🤷 Unknown	1
	2024-02-17	TLS/SSL Crawler	activity	🤷 Unknown	1
	2024-02-16	TLS/SSL Crawler	activity	🤷 Unknown	1
□	2024-02-13	SSH Bruteforcer	worm	❌ Malicious	1
	2024-02-13	Masscan Client	tool	🤷 Unknown	1

Number of intention flips: 50

▶ Details

🟩 benign 🟥 malicious ⬛ unknown

WE NEED

TO TALK

ABOUT

KEV

It Has Been

1

Days Since The
Last KEV Release

https://kev.hrbrmstr.app

https://www.cisa.gov/known-exploited-vulnerabilities-catalog

CVE-2019-7256: Nice Linear eMerge E3-Series OS Command Injection

CVE-2021-44529: Ivanti Endpoint Manager Cloud Service Appliance (EPM CSA) Code Injection

CVE-2023-48788: Fortinet FortiClient EMS SQL Injection