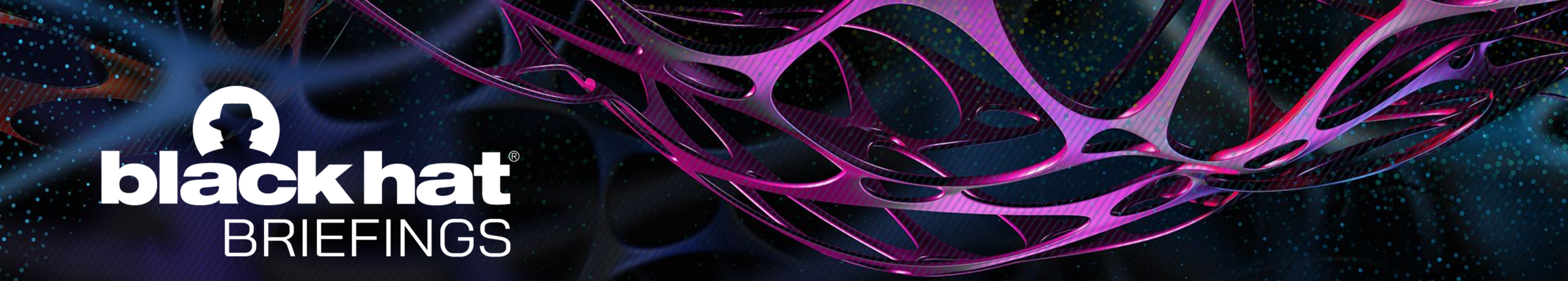


AUGUST 6-7, 2025

MANDALAY BAY / LAS VEGAS

Vulnerability Haruspicy

Picking Out Risk Signals from Scoring System Entrails

Tod Beardsley, runZero VP of Security Research and CVE Mucker-Abouter

Oracular Methods for Quantifying Risk

Haruspicy: What is it anyway?

A brief jaunt into deriving signals from entrails, specifically, sheep livers

CW: Meat

CVSS: Casting fractal shadows

The oldest current system, the Common Vulnerability Scoring System

EPSS: ML-based magicks

A relative newcomer, the Exploit Prediction Scoring System

CW: AI

SSVC: Tarot for your criticality

The decidedly un-mathy Stakeholder-Specific Vulnerability Categorization decision tree

Haruspicy: A Brief Primer

Haruspicy was favored by the Etruscans, and also used by Assyrians, Babylonians, and other early Mediterranean and African cultures.

Image source:
https://www.queens.ox.ac.uk/news/reading-the-past-ancient-liver-divination/

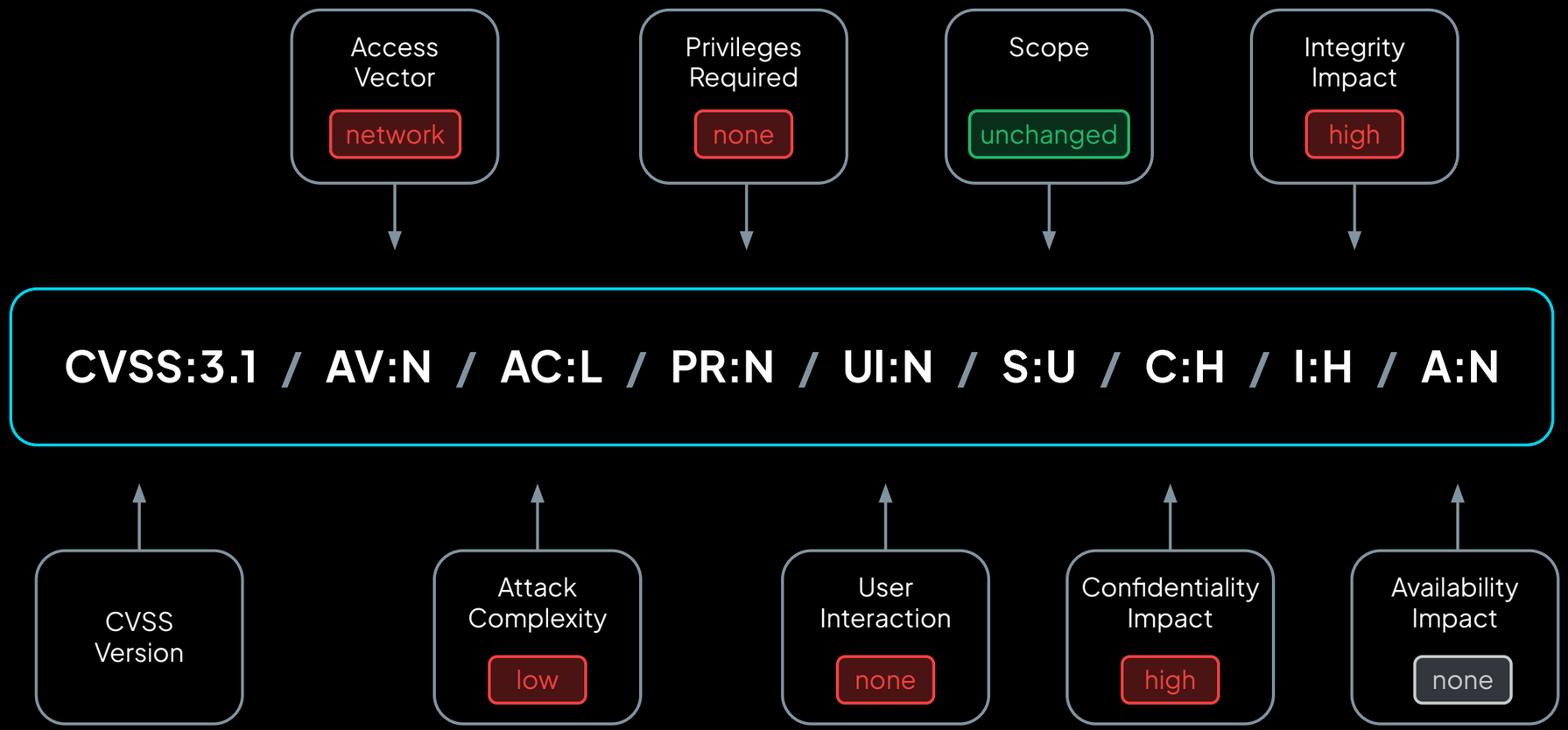
- The gods would reveal their will through omens, manifested in the entrails of sacrificial animals – particularly the liver.
- References on thousands of favorable and unfavorable omens were maintained by practitioners.
- Balancing these omens gets you an answer to your specific question.
- Take random signals, and assert that they're not random. The original P-Hackers!

CVSS: The Only Number Anyone Cares About

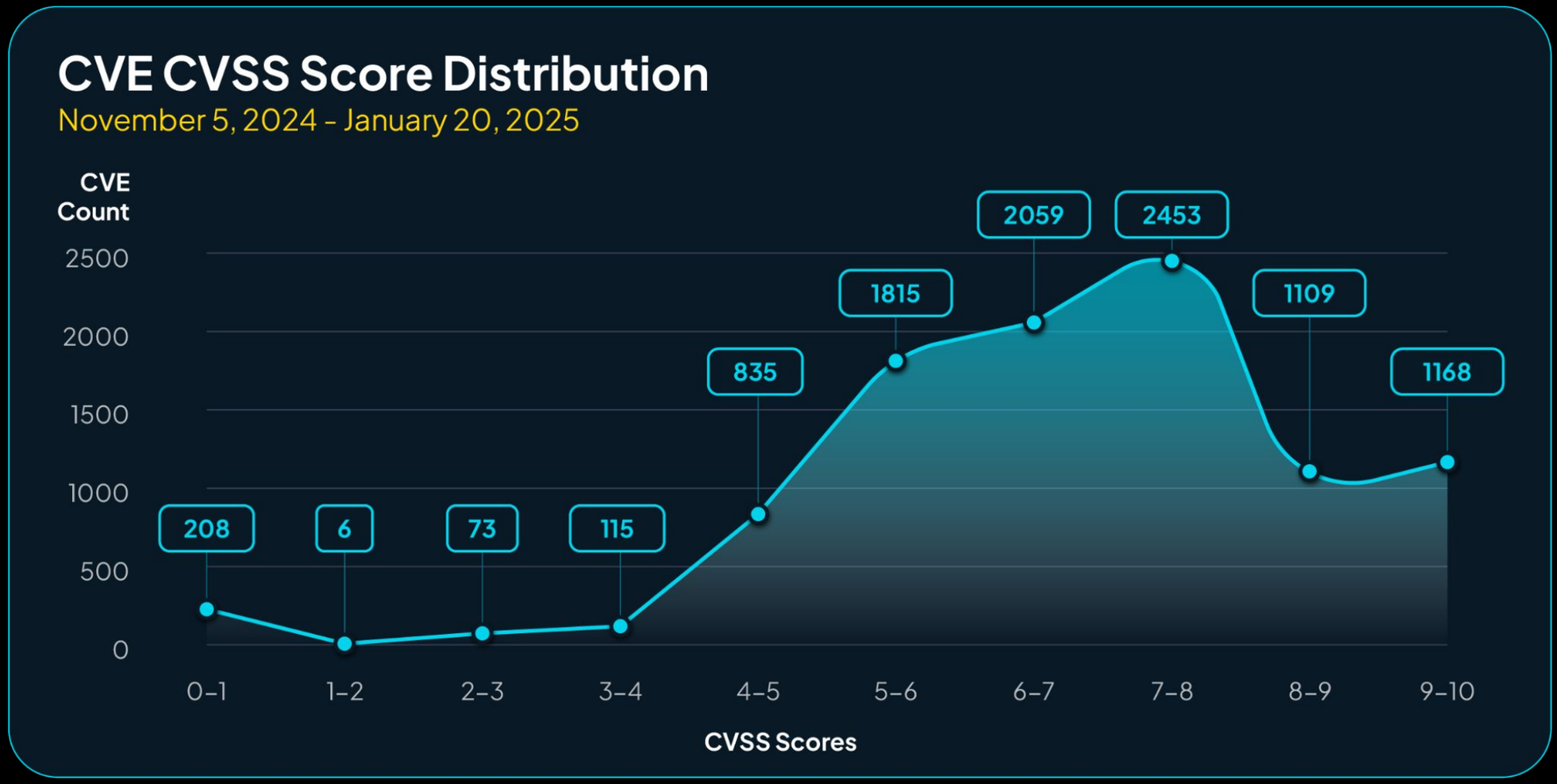
The Common Vulnerability Scoring System has emerged as a bedrock of risk ratings and vulnerability scoring.

- Eight vectors are commonly used, describing various aspects of the vulnerability.
- You don’t strictly need CVE to do this.
- Version 4 gives more fidelity to the 3.1 notion of “scope.”
- Great for checkbox-based security decision making.
- Also great for tech news headlines when it’s 9.8/10.0.

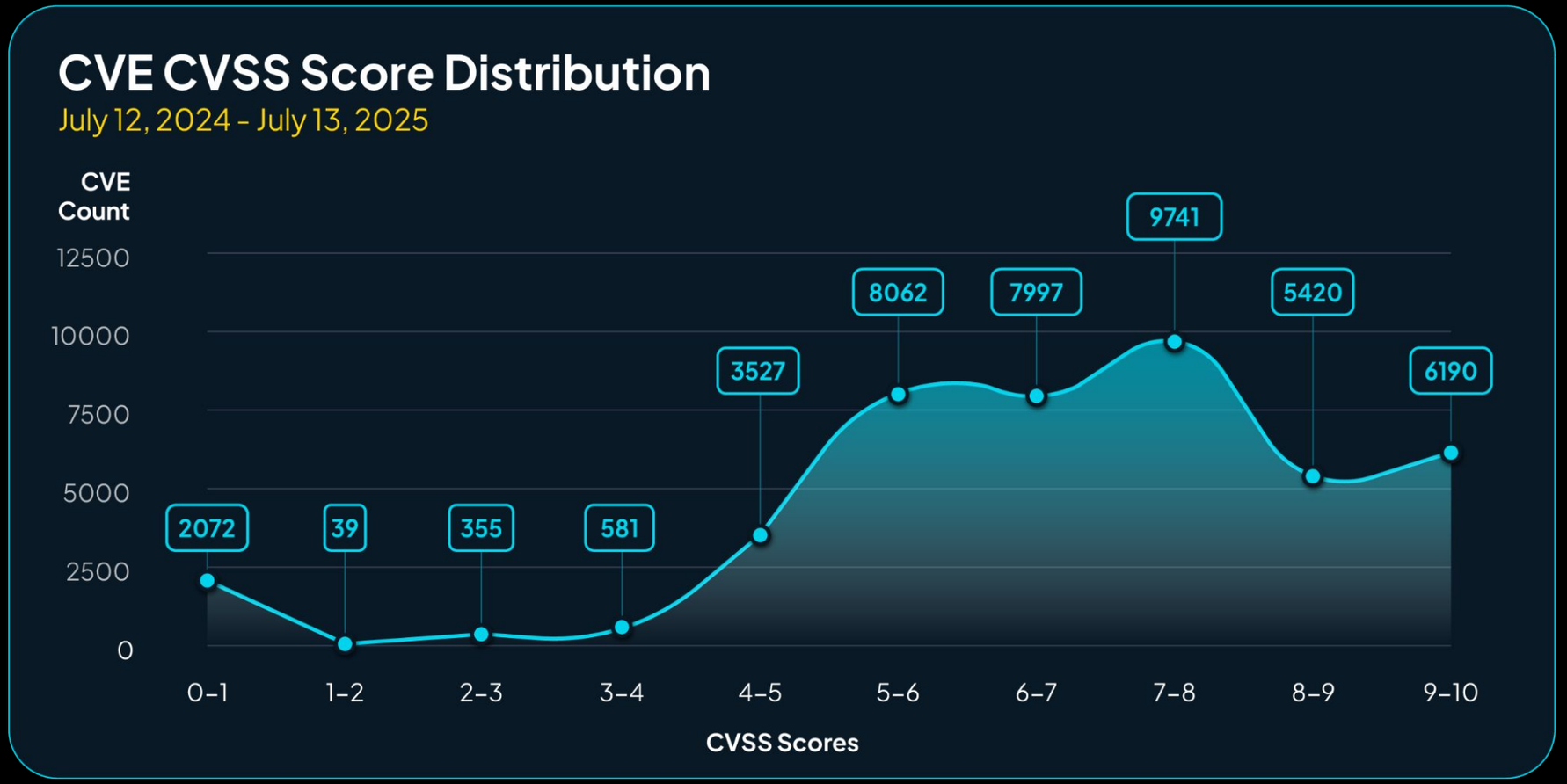
CVSS: Example CVSS Score 9.1 (Critical)



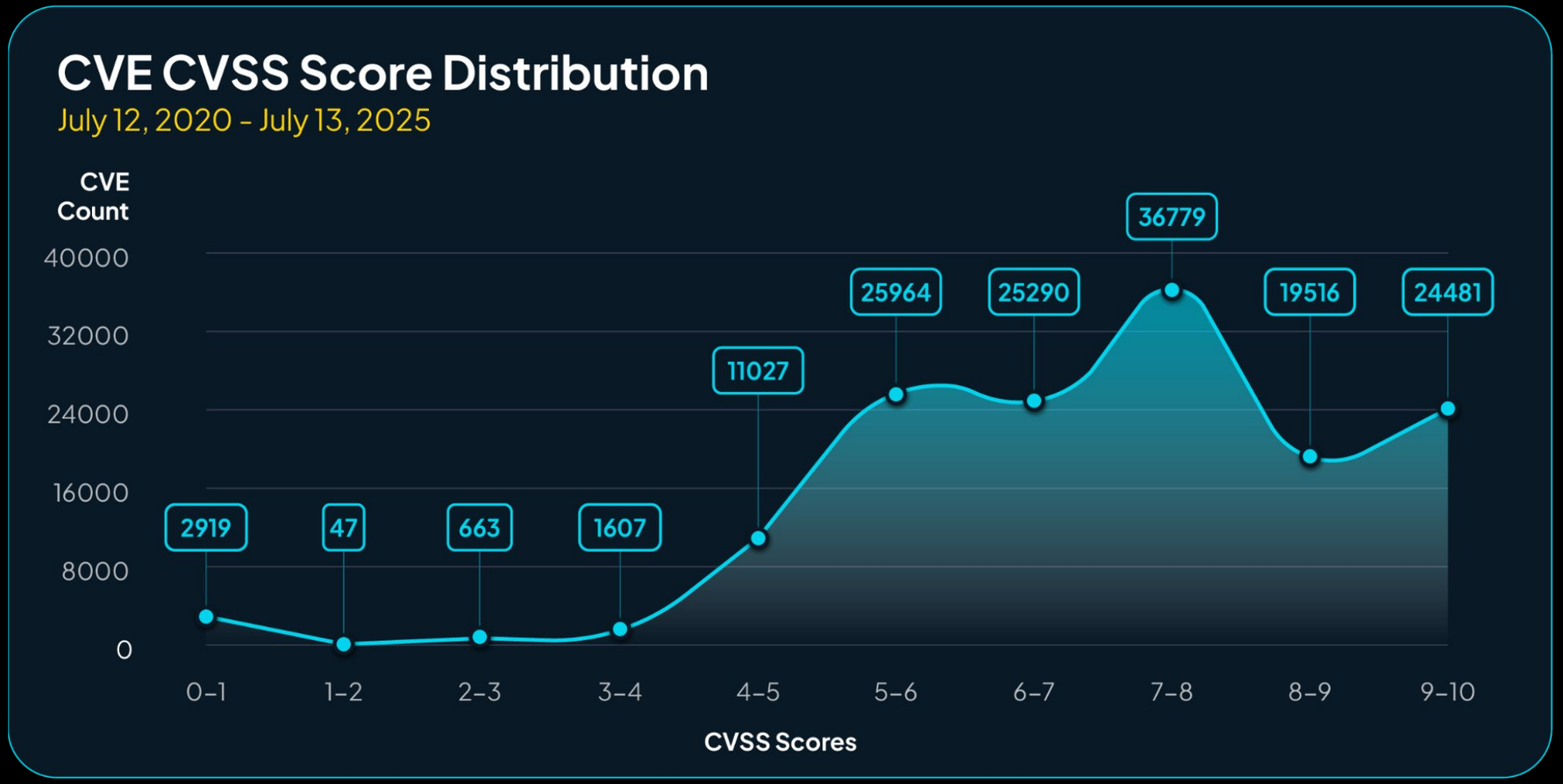
CVSS: Weirdly Predictable Distributions



CVSS: Weirdly Predictable Distributions



CVSS: Weirdly Predictable Distributions



CVSS: Casting Fractal Shadows

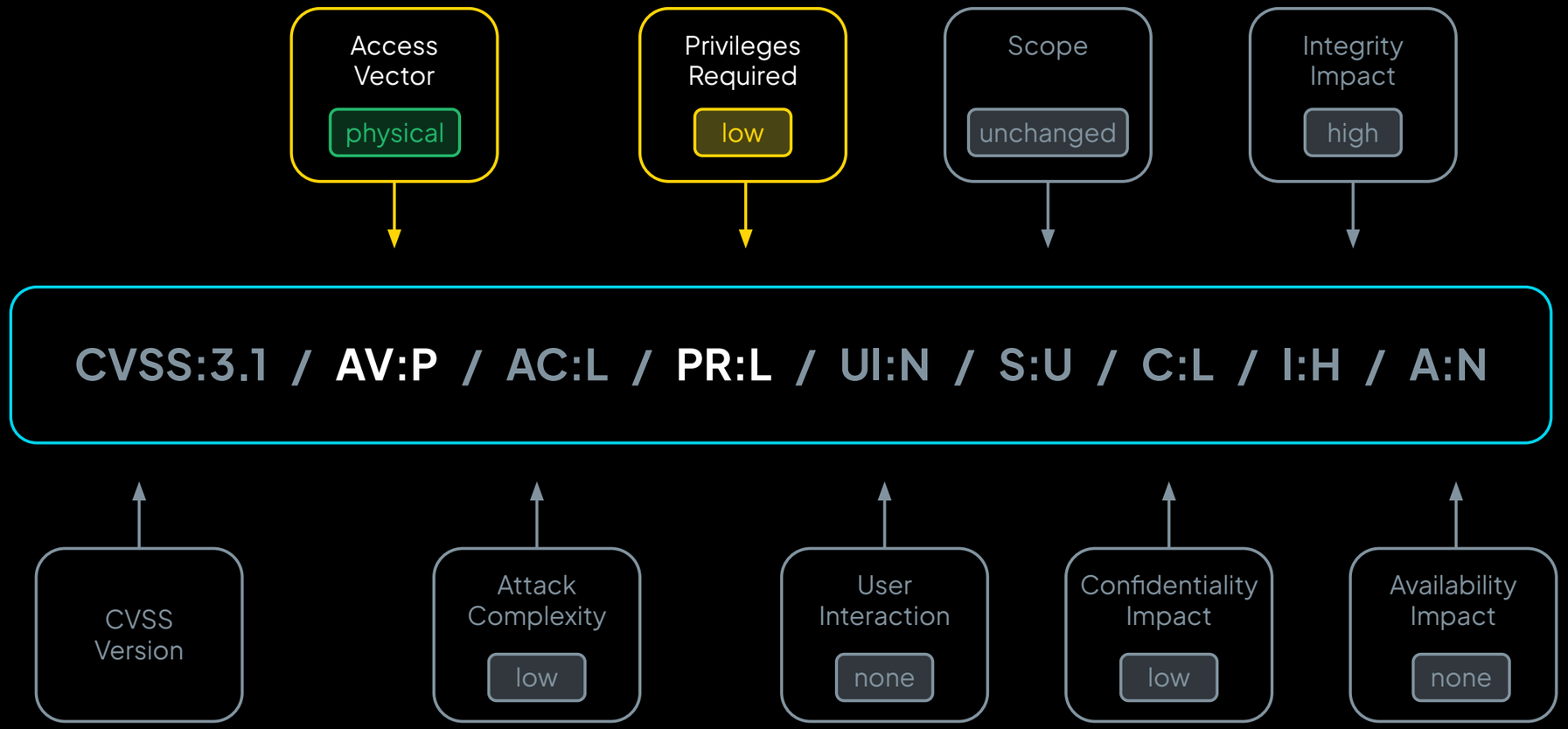
CVSS is great at **measuring itself.**

Image source:
https://becomingborealis.com/jan-saenredam-the-allegory-of-the-cave/

- Given any time scale, the distribution of CVSS scores appears to be consistent.
- There is a suspicious lack of low to medium severity vulnerabilities.
- These patterns persist today, implying that we're still writing high-severity bugs at the same rate we always have.
- The vectors are where the action's at.

CVSS: Example CVSS Score 5.9

CVE-2025-4382



black hat BRIEFINGS

PVSS: More of the same?

François Proulx's

"Living Off the Pipeline"

ATTACK VECTOR
- **Public Repo** (OSS)
- **Public Repo** (Second Order)
- **Private Repo**
- **On Premise** (SCM/CI/CD)

ATTACK COMPLEXITY
- **Low**
- **High**

PRIVILEGES REQUIRED
- **Normal**
- **Low**
- **High**

USER INTERACTION
- **None**
- **Passive**
- **Active**

SCOPE
- **High**
- **Unchanged**

CONFIDENTIALITY
- **High**
- **Low**
- **None**

INTEGRITY
- **High**
- **Low**
- **None**

AVAILABILITY
- **High**
- **Low**
- **None**

SEVERITY SCORE VECTOR **Critical** 9.5 **PVSS:1.0 / AV:N / AC:L / PR:N / UI:N / S:U / C:H / I:H / A:N**

AIVSS: More of the same?

OWASP's

"Agentic AI VSS"

The first comprehensive framework for assessing and scoring vulnerabilities in agentic AI systems.
Built on OWASP principles with industry-standard scoring methodology.

AIVSS Calculator

Real-time vulnerability scoring with detailed metrics and impact assessment.

OWASP Top 10

Critical security risks specifically designed for agentic AI systems.

Industry Standard

Standardized methodology for consistent vulnerability assessment.

EPSS: Machine learning, algorithmic, and occult

The Exploit Prediction Scoring System was first released in April of 2021, and has “prediction” right in the name.

- Easiest to think of as having “right” and “left” sides.
  - CVSS vectors, keywords in descriptions, number and types of references, KEV presence, hacker chatter.
  - Honeypot hits, IDS/IPS alerts, EDR events, cybersecurity vendor feeds (Fortinet, GreyNoise, ShadowServer, and more).
- Agnostic on specific vulnerability qualities.
- Produces probabilities, not ratings, per se.

EPSS: But What is Exploitation Activity

EPSS predicts something like 10,000 or so unique CVEs to be exploited per month. **This is wildly high.**

But this is explained by a specific definition of “exploitation activity.”

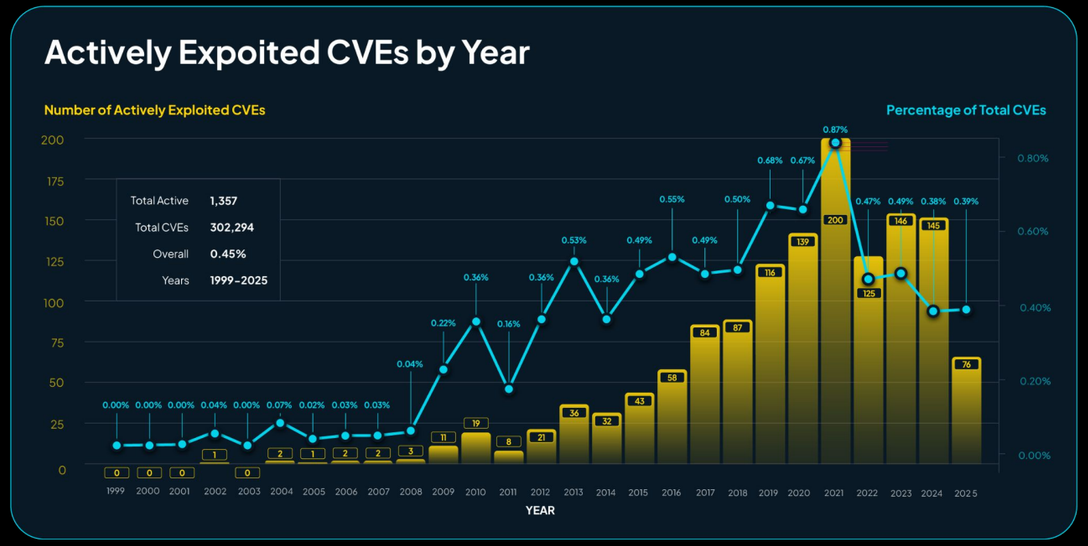
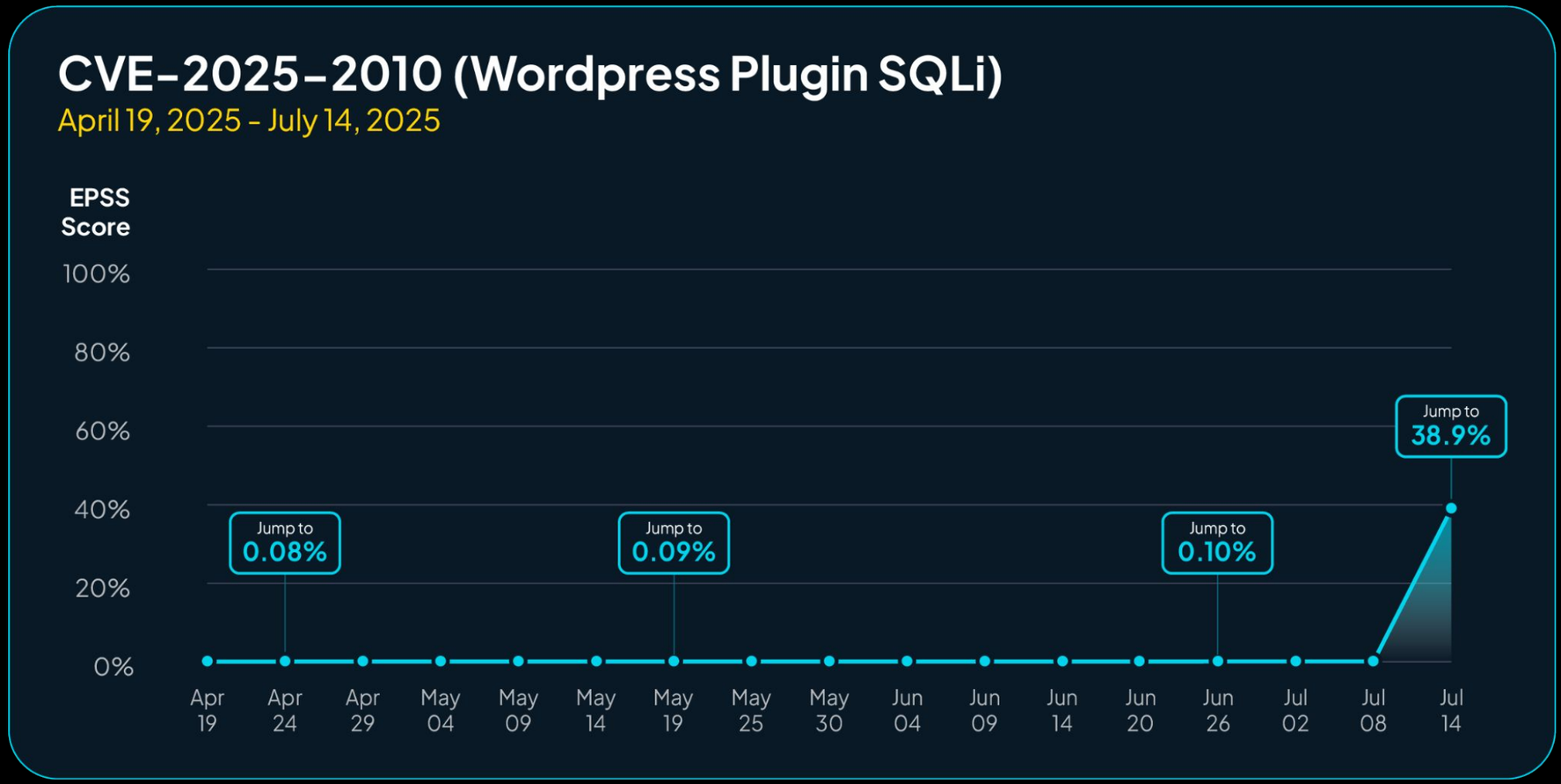


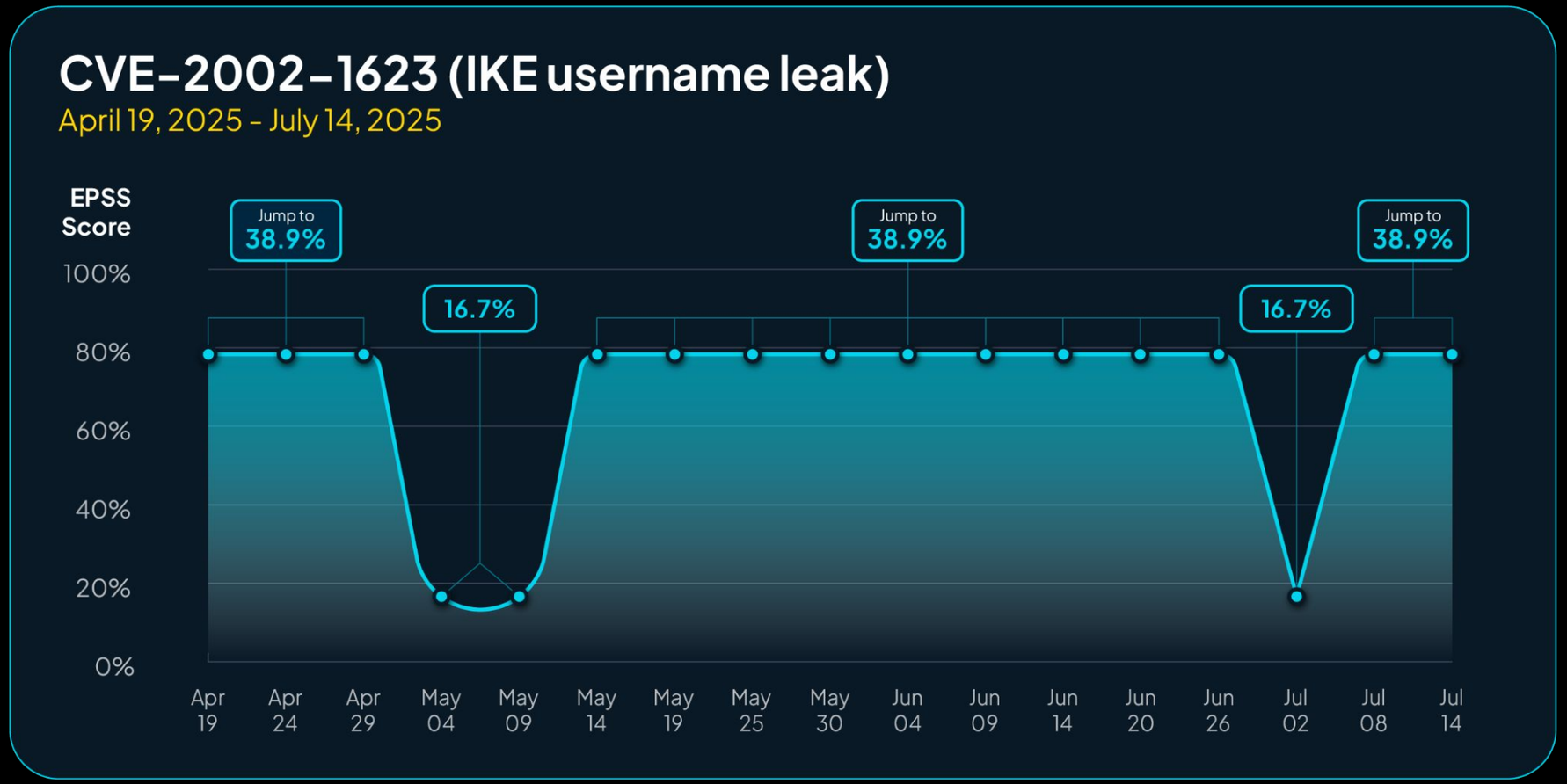
Image source:
https://cvedata.com/#active_exploitation_by_year

- CISA KEV has a total of ~1400 actively exploited vulnerabilities, over several years.
- Exploitation “activity” is not limited to shells or exfils.
- Noisy, obvious activity will tend to push EPSS scores up.

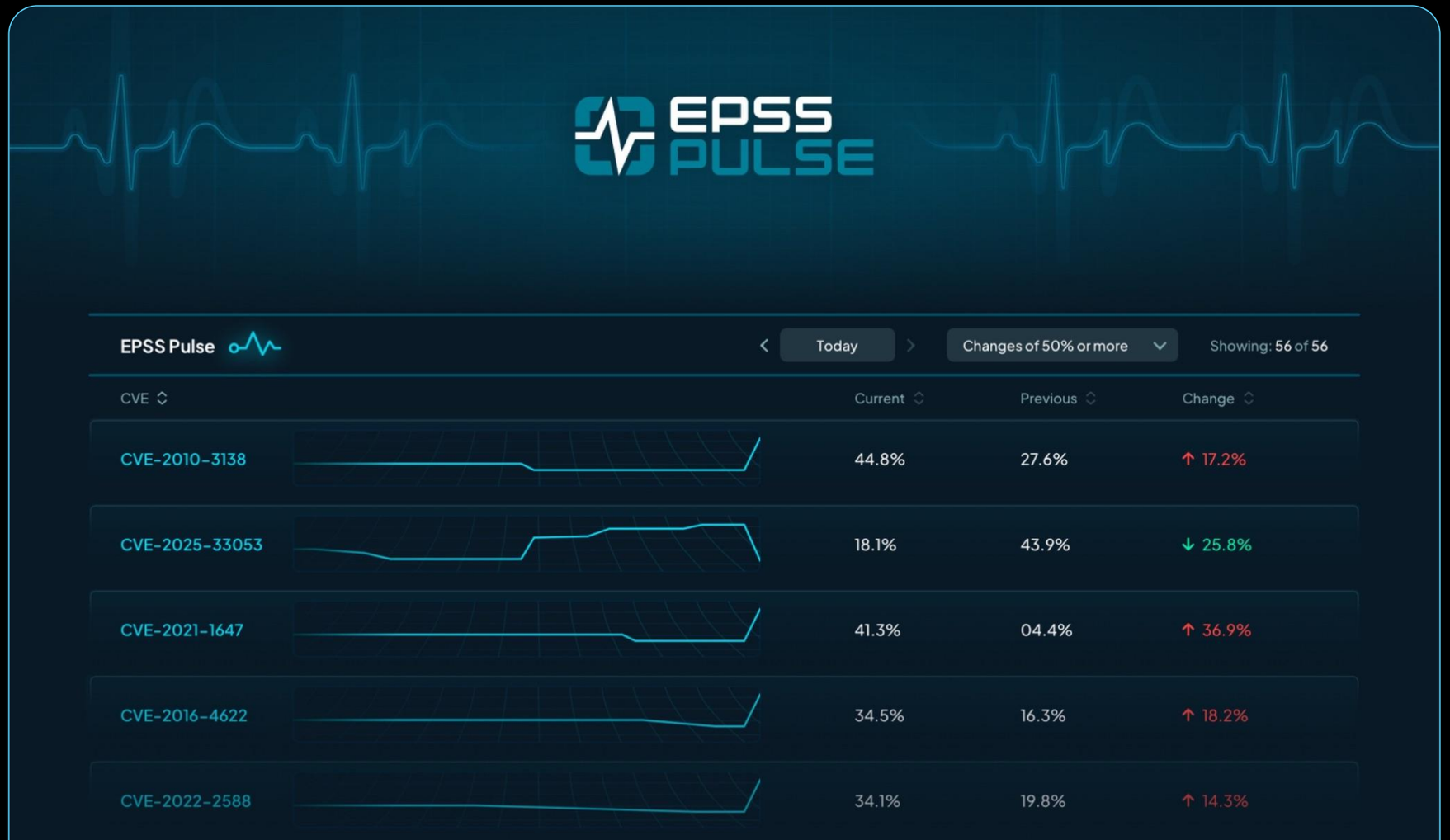
EPSS: Example EPSS Jumper



EPSS: Example Volatile EPSS



EPSS: Pulse!


EPSS PULSE
EPSS Pulse
Today
Changes of 50% or more
Showing: 56 of 56
CVE
Current
Previous
Change
CVE-2010-3138
44.8%
27.6%
↑ 17.2%
CVE-2025-33053
18.1%
43.9%
↓ 25.8%
CVE-2021-1647
41.3%
04.4%
↑ 36.9%
CVE-2016-4622
34.5%
16.3%
↑ 18.2%
CVE-2022-2588
34.1%
19.8%
↑ 14.3%

EPSS: Pulse!

Play along at home: Watch daily major-movers on EPSS with EPSS Pulse!

- Free, ungated web app that provides a handy dashboard for those CVEs that change a lot in one day. Also, RSS!
- Still not super sure if this is a valuable indicator, but the last several weeks have been pretty promising.
- https://www.runzero.com/epss-pulse
- Very interested in the detective work you do!

EPSS: “Likely” Exploited Vulnerabilities (LEV)

LEV seeks to answer the question, “Why are KEV lists so short?”

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

- A well-reasoned, mathematically sound foundation for framing the question. Definitely worth the read.
- Unfortunately, no particularly good answers quite yet, since we cannot yet observe all of cyberspace.
- “[LEV] inevitably has a margin of error which is currently unknown.”
- If you want to help, talk to Jono and Peter!

SSVC: Decision Tree for Action

While EPSS looks at thousands of data points per vulnerability,
The Stakeholder-Specific Vulnerability Categorization asks the question,
“what if we just did, like, five?”

- SSVC is very context-aware of your environment.
- Not technically a scoring system, but a decision tree.
- Ends in (site-defined) actions: Track, Monitor, Attend, and Act.
- Provides a starting point for more customization by domain.
- Roughly mappable to severity, but only if you’re going to do something about it.

SSVC: Decision Tree for Action

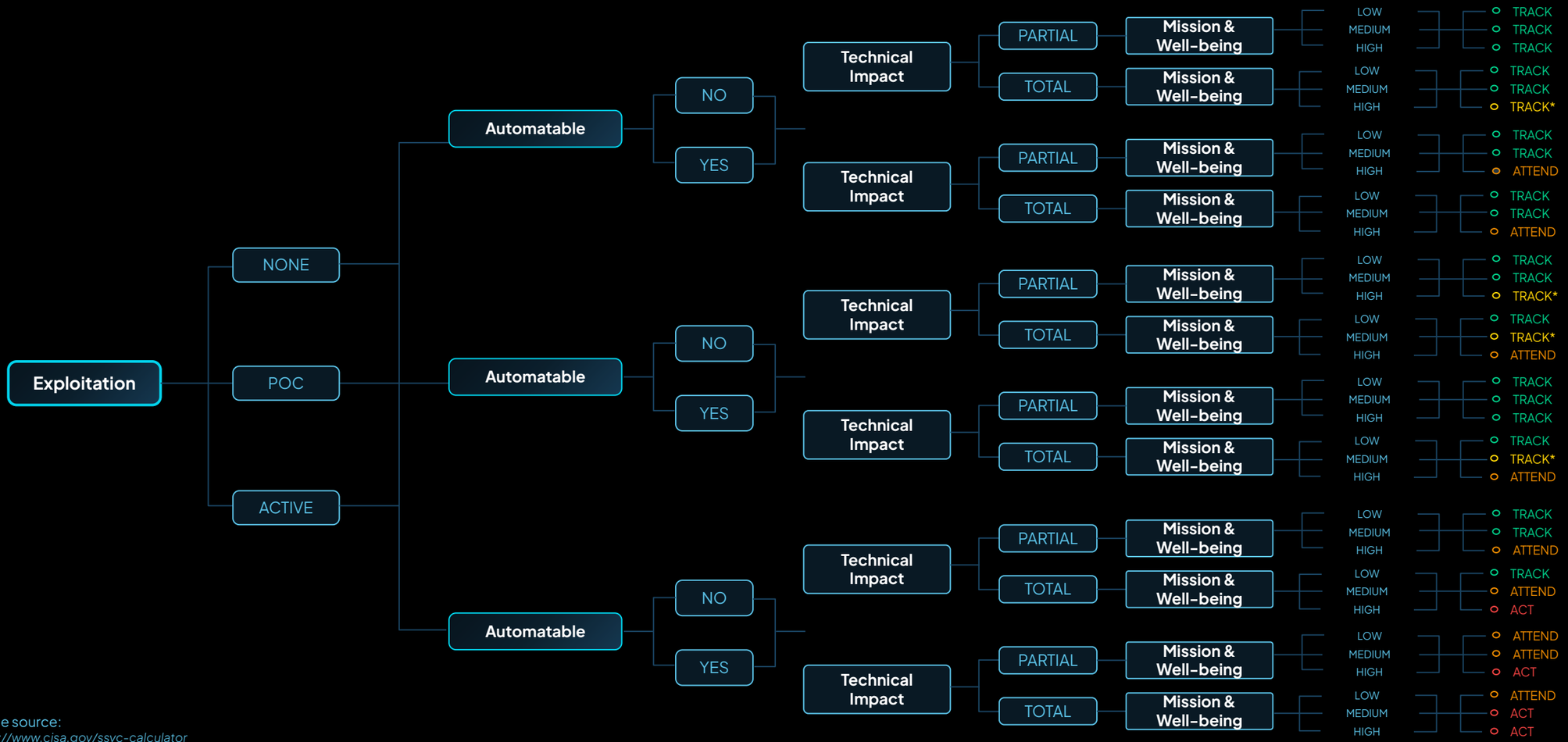


Image source:
https://www.cisa.gov/ssvc-calculator

SSVC: Decision Tree for Action

- Is there active exploitation? Or a known exploit?
- Does an exploit need any help?
- What's the technical impact of an exploit?
- How important are the targets?
- Are people going to die?

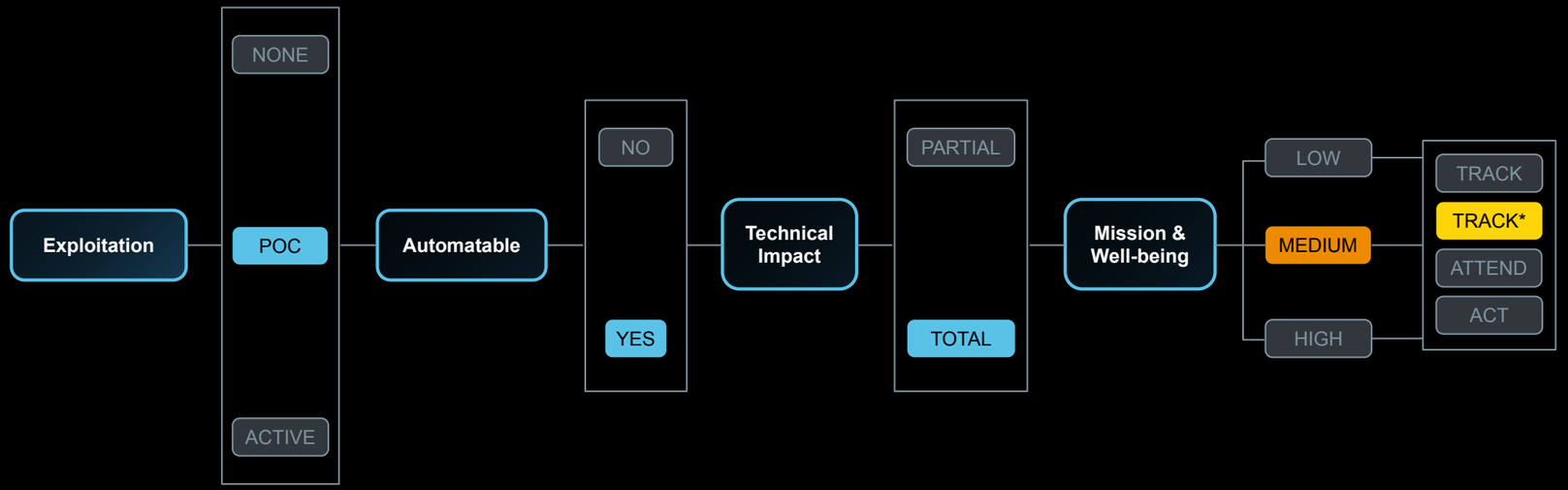


Image source:
https://www.cisa.gov/ssvc-calculator

SSVC: Tarot for your Environment

SSVC is admittedly – even proudly – squishy, but it's useful for expressing "what's next" and getting your stakeholders either panicky or chilled out. And today, some of the hard parts are now done for you!

Image source:
https://pixabay.com/photos/craft-tarot-divination-2728227/

- CISA-ADP (aka Vulnrichment) now provides exploitation evidence directly on CVE records.
- Also provided is technical impact.
- Triaging from those two basic qualities gets you to about 400 vulnerabilities to review, today.
- It's still on you to assess your own environment, and to define what actions flow from each of the decisions.

The Real Vulnerability Scoring System

The friends we made along the way.

Scoring systems can give some guidance, but none are reliably mechanistic.

Image source:
https://www.computerhistory.org/collections/catalog/102645279

- While all three scoring systems provide useful signals, they're not quite as obvious as they'd like to be.
- LLMs, ML, and other things labelled "AI" can be useful.
- Human experts are still required for judgement.
- No scoring system can predict human motivation.
- KEVs, trust groups, continuous monitoring, and a historical sensibility are your best sources of truth.

black hat BRIEFINGS

Thank You! Now Do Some Homework!

New Report

DIVINING RISK

Deciphering Signals from Vulnerability Scores

CVSS EPSS SSVC

See what CVSS, EPSS, and SSVC get right, where they fall short, and how to turn that insight into smarter prioritization.

Tod Beardsley

VP of Security Research

Find me on the internet and share how you rate vulnerabilities!

https://infosec.exchange/@todb

EPSS PULSE

Play Along At Home! Check out runZero's EPSS Pulse tracker and see if you can get ahead of the next one.