BSIDES Dublin

Complexities of Vulnerability Management

Strategies for Prioritizing and Remediating Security Holes

About Me

Sr. Engineering Manager @ CrowdStrike

Solving Problems and Breaking things

Twitter: @ramospablo

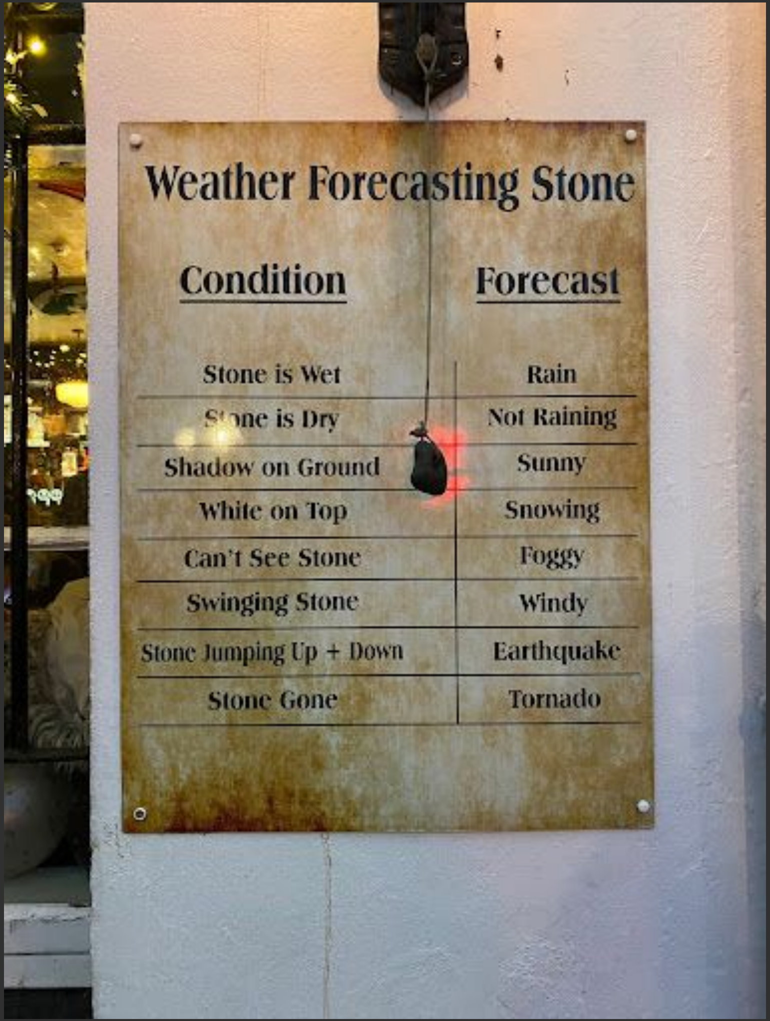
Image: https://labs.openai.com/s/Im5yDDLR0EBwrn9x64Ywicxn

Vulnerability Management

Detection	Accuracy	Actions
What and How Many	Triaging and FP/FNs	What you do

Reality Check

There is no silver bullet



Weather Forecasting Stone

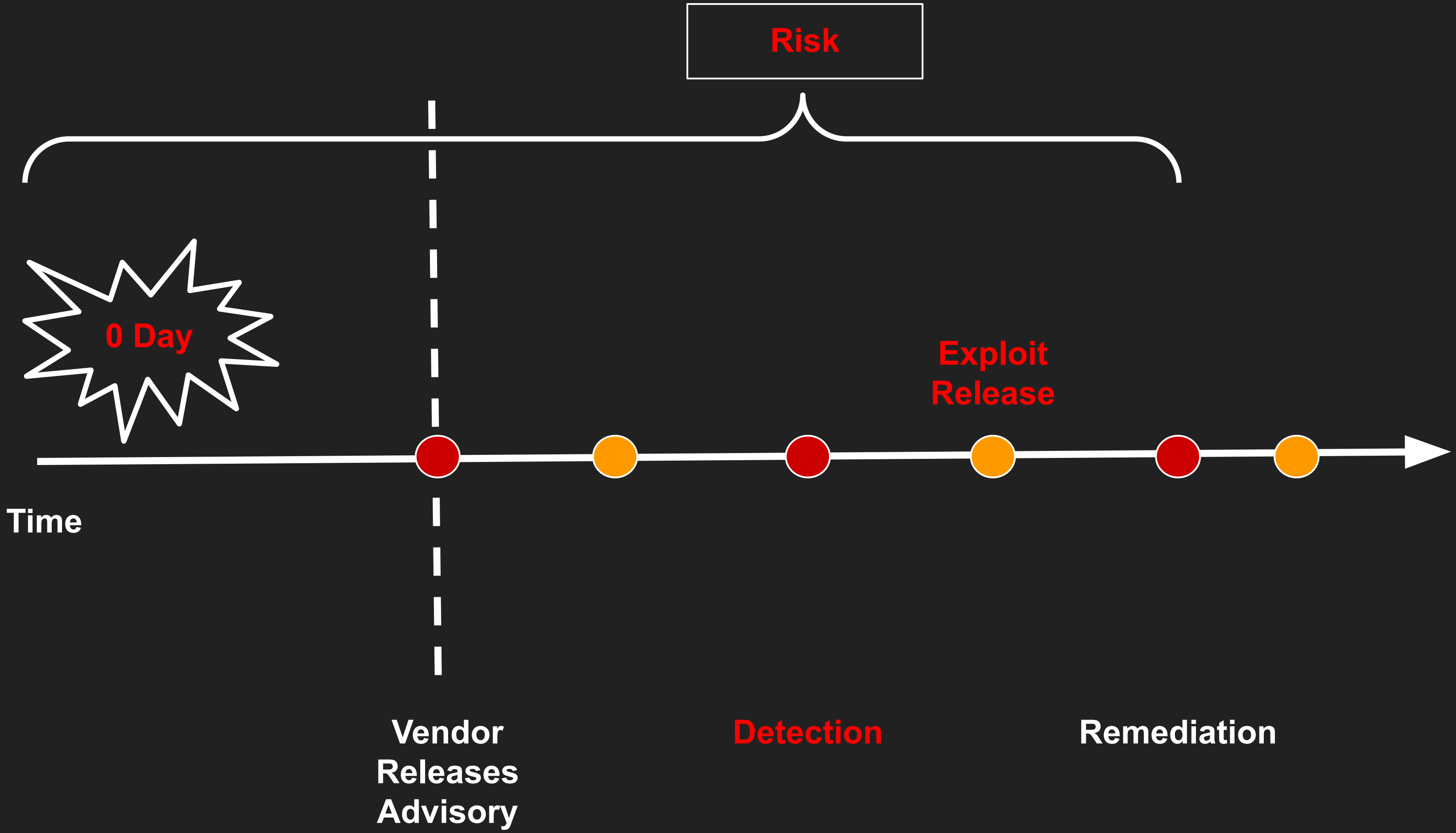
Condition	Forecast
Stone is Wet	Rain
Stone is Dry	Not Raining
Shadow on Ground	Sunny
White on Top	Snowing
Can't See Stone	Foggy
Swinging Stone	Windy
Stone Jumping Up + Down	Earthquake
Stone Gone	Tornado

All the things you have

Vulnerabilities

Is it complex?

Image: https://labs.openai.com/s/Tk9Vxb3GLUpObGPquXCSUi1r


Risk
0 Day
Exploit Release
Time
Vendor Releases Advisory
Detection
Remediation

Time to Awareness

How fast you become aware of something new affecting your

Time to Detection

How much it passes until you get a report with a new finding

Time to Remediation

Once you know, how fast you’re able to fix the problem

Detections

There are **many** vulnerabilities. Which ones you care about?

CVEs

CVE, Exploits and More

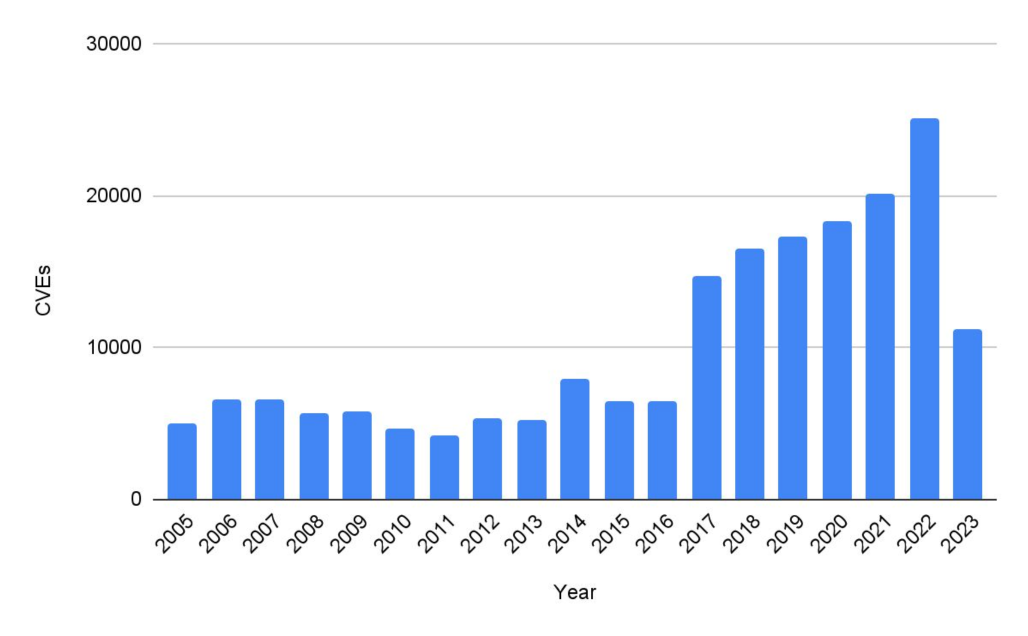
EOL

A silent risk

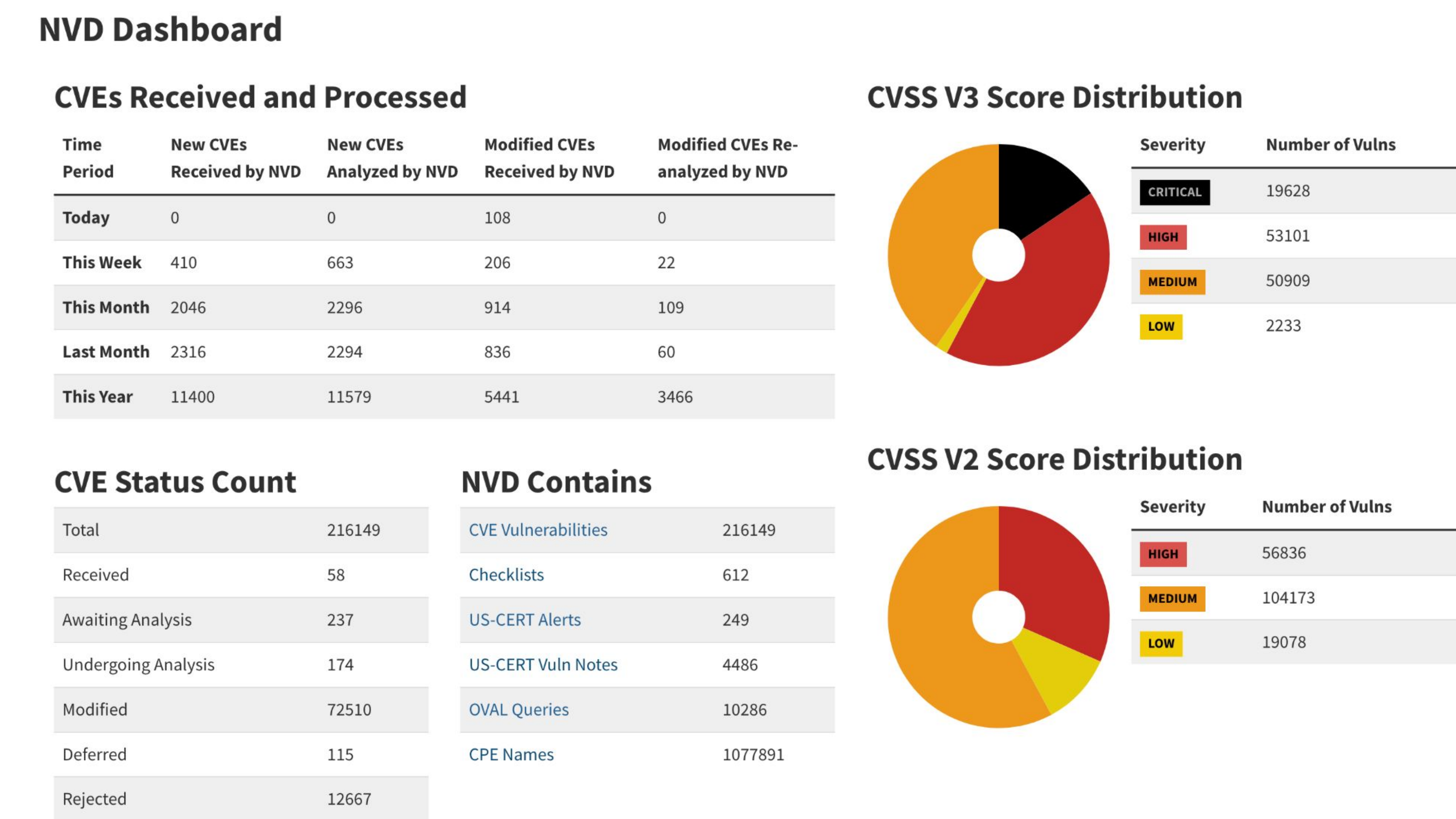
Others?

It’s not a CVE.
It’s a feature

CVEs released every year



- You can’t detect them all
- You can’t patch them all
- CVEs Numbers is not the only challenge



NVD Dashboard

CVEs Received and Processed

Time Period	New CVEs Received by NVD	New CVEs Analyzed by NVD	Modified CVEs Received by NVD	Modified CVEs Re-analyzed by NVD
Today	0	0	108	0
This Week	410	663	206	22
This Month	2046	2296	914	109
Last Month	2316	2294	836	60
This Year	11400	11579	5441	3466

CVSS V3 Score Distribution

Severity	Number of Vulns
CRITICAL	19628
HIGH	53101
MEDIUM	50909
LOW	2233

CVE Status Count

Total	216149
Received	58
Awaiting Analysis	237
Undergoing Analysis	174
Modified	72510
Deferred	115
Rejected	12667

NVD Contains

CVE Vulnerabilities	216149
Checklists	612
US-CERT Alerts	249
US-CERT Vuln Notes	4486
OVAL Queries	10286
CPE Names	1077891

CVSS V2 Score Distribution

Severity	Number of Vulns
HIGH	56836
MEDIUM	104173
LOW	19078

Exploits and Vulnerabilities

Actively Exploited

Malicious activity related to the exploit has been reported

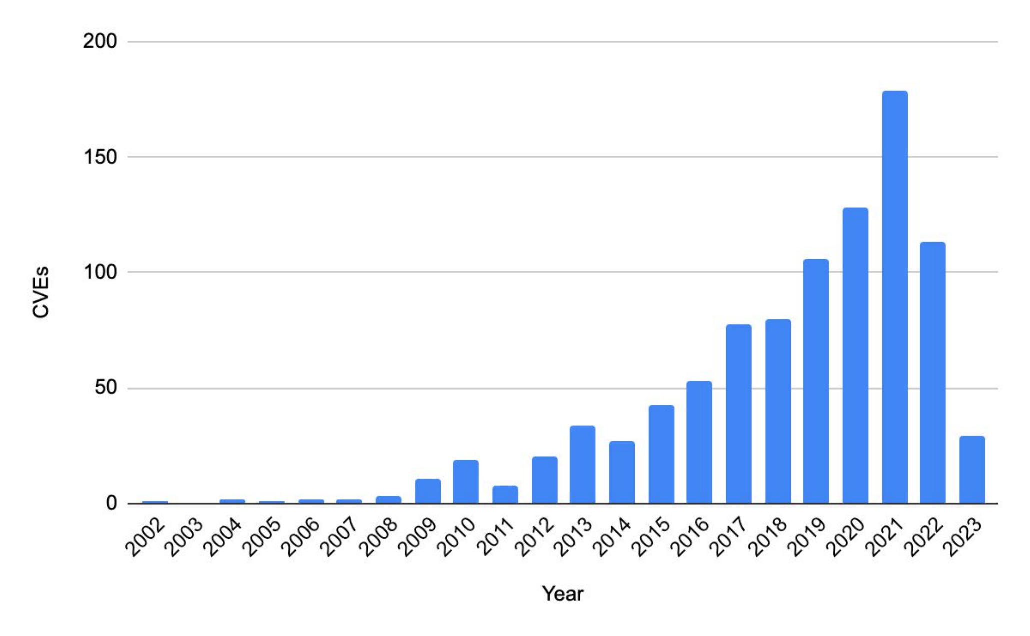
Exploit Available

It exist but no “confirmation”

PoC

Not functional but some work is out there

CISA KEV CVEs by Year



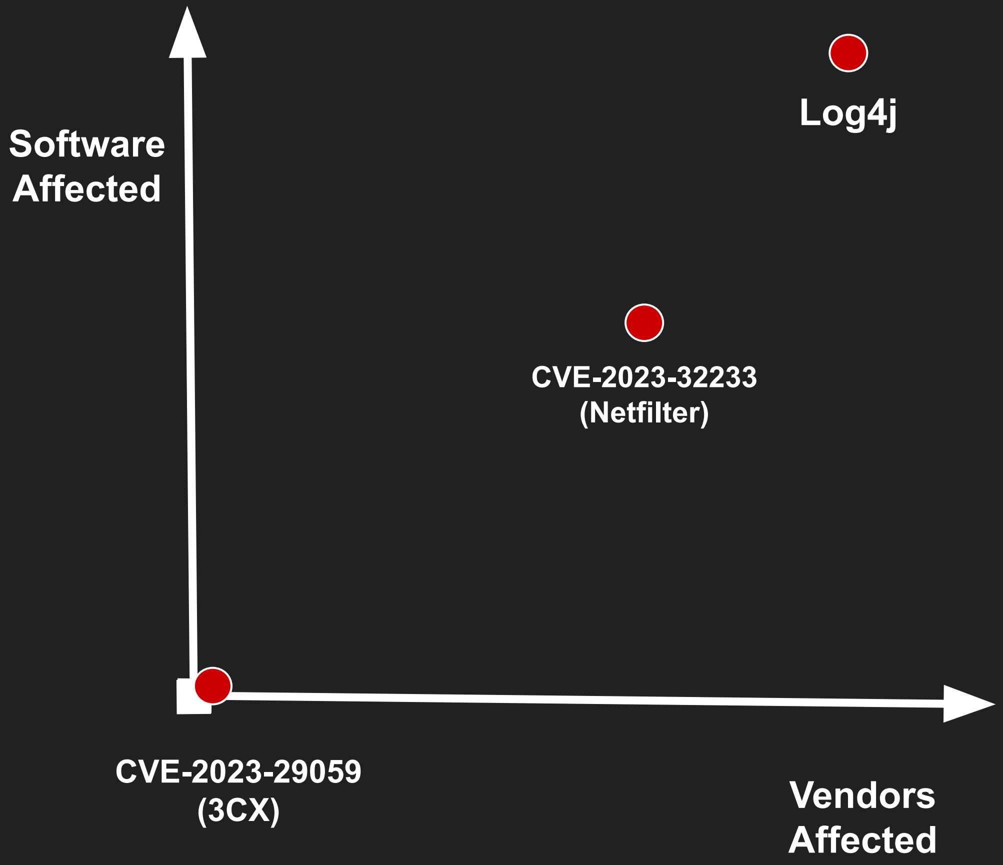
Vendor	CVEs
Microsoft	259
Cisco	63
Adobe	60
Apple	54
Google	47
Oracle	32
Apache	28
VMware	16
D-Link	13
Linux	12
Citrix	11
Mozilla	10
SAP	10
Fortinet	10
QNAP	10

0.46%

Of “known” Vulnerabilities have been flagged as Exploited by CISA

Detection does not imply Coverage

How many thing are affected?



- Multiple Products affected
- Multiple Platforms affected
- Everything is affected!

How to fight back?

Putting everything together

Image: https://labs.openai.com/s/a7zsGho77tbB46Rg3SxQWeUC

Context!

Your environment is unique but with similarities

Asset

What it is and where

Controls

Prevention and Protection

Risk

What happens if it’s compromised

Prioritisation

What do you do next?

CVSS

VS

Dynamic Models (ML/AI)

Guidance

Getting to a resolution

Update to the latest available version

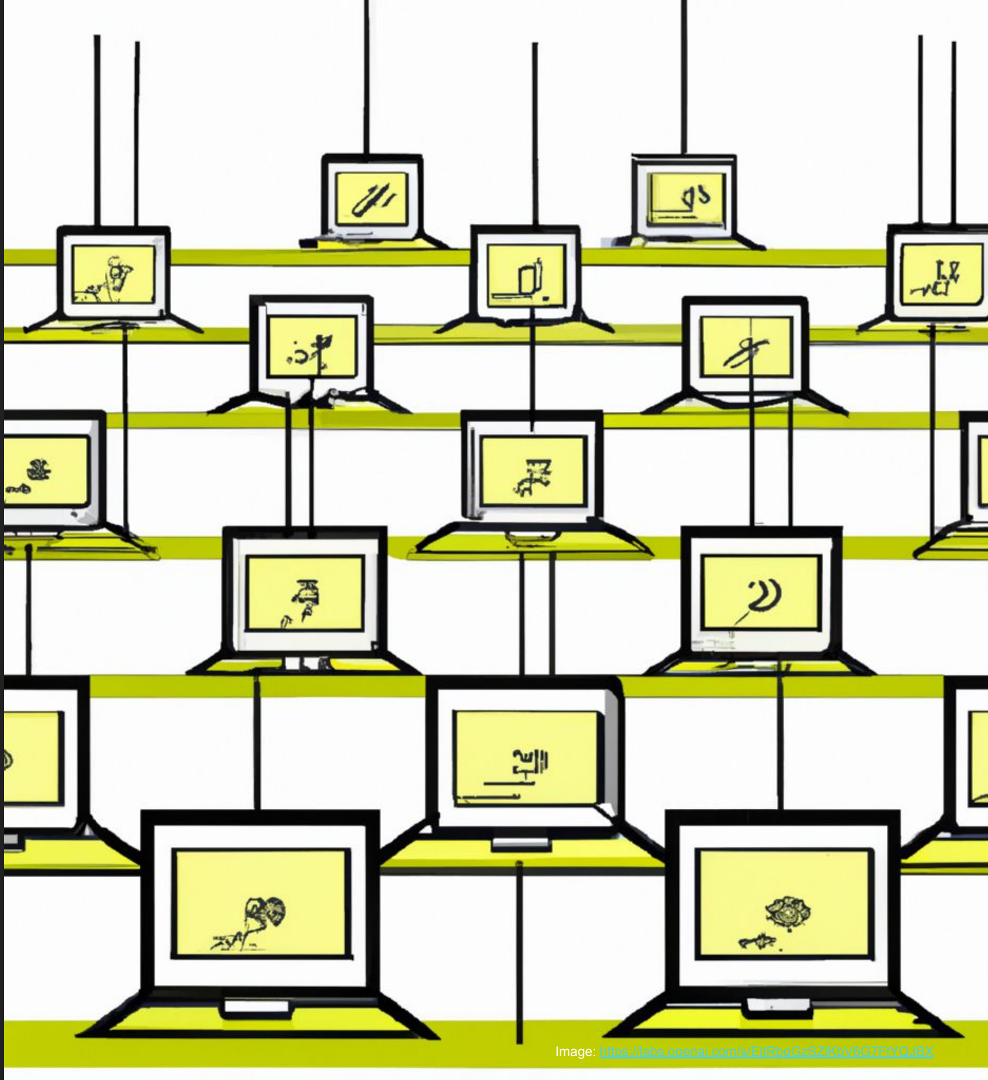


Image: https://labs.openai.com/s/EjtRbqGzSZlKbV6G7FtYQJBX

Detection	Accuracy	Actions
Context	Prioritisation	Remediation

Solutions?

Flexibility, accountability and actionability

Prioritisation and Remediation

- Build on processes and Iterate
- Focus on Remediation and Protection
- Combine Tools + People + Processes
  - SBOMs, VEX and More

Image: https://labs.openai.com/s/xs4H5MMxgel708Tk0tlMJLlq

Thank you!

No solutions provided, more context required

Q&A

BSIDES Dublin