Navigating the Challenges of Risk-Based Vulnerability Management in a Cloud-Native World

Practitioner to Practitioner suggestions to fight modern VM in modern AI world

James Berthoty - Security Engineer Latio Tech

Nate Sanders – Bazaarvoice – Head of Security Engineering

Francesco Cipollone, Co-Founder Phoenix Security, fc@phoenix.security

PHOENIX SECURITY

Warning revelation ahead

Warning

About the speakers

2025 CVE/FIRST VulnCon

LinkedIn Profile

Francesco Cipollone

CEO & Co-Founder Security Phoenix, Board CSA UK

James Berthoty

The New Nate Security Engineer

Austin Hackers

uvehed

You can argue with people, but you can’t argue with data

Data driven approach can help making compelling arguments

Agenda

Intro & Context

Current Scenario : 2015 to today – SLA, Critical, CVSS which one to choose

P1 - Challenges in prioritization with old metrics a practitioner story

P2 - Prioritizing right – from code to cloud what matters and how to declutter the noise

P3 – Threat Centric approach on vulnerability for prevention

Conclusion & Q&A

Hands up if ..

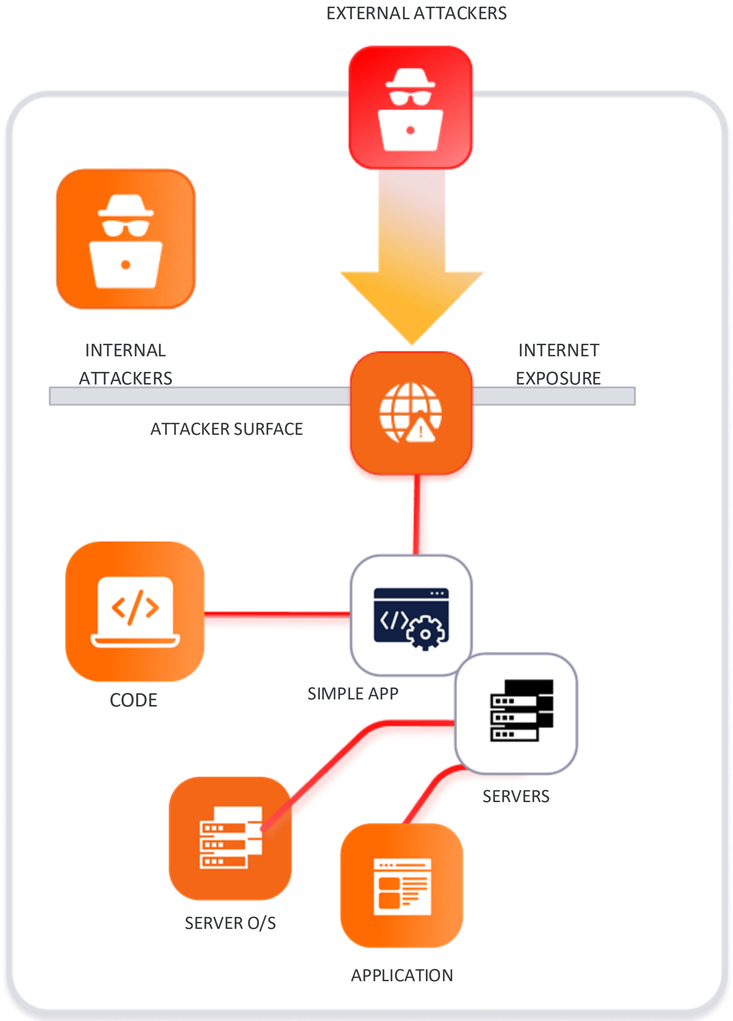
You believe your company has a functional vulnerability management program

You believe it covers all areas and scope of vulnerabilities

You are prioritizing all findings equally by normalized risk

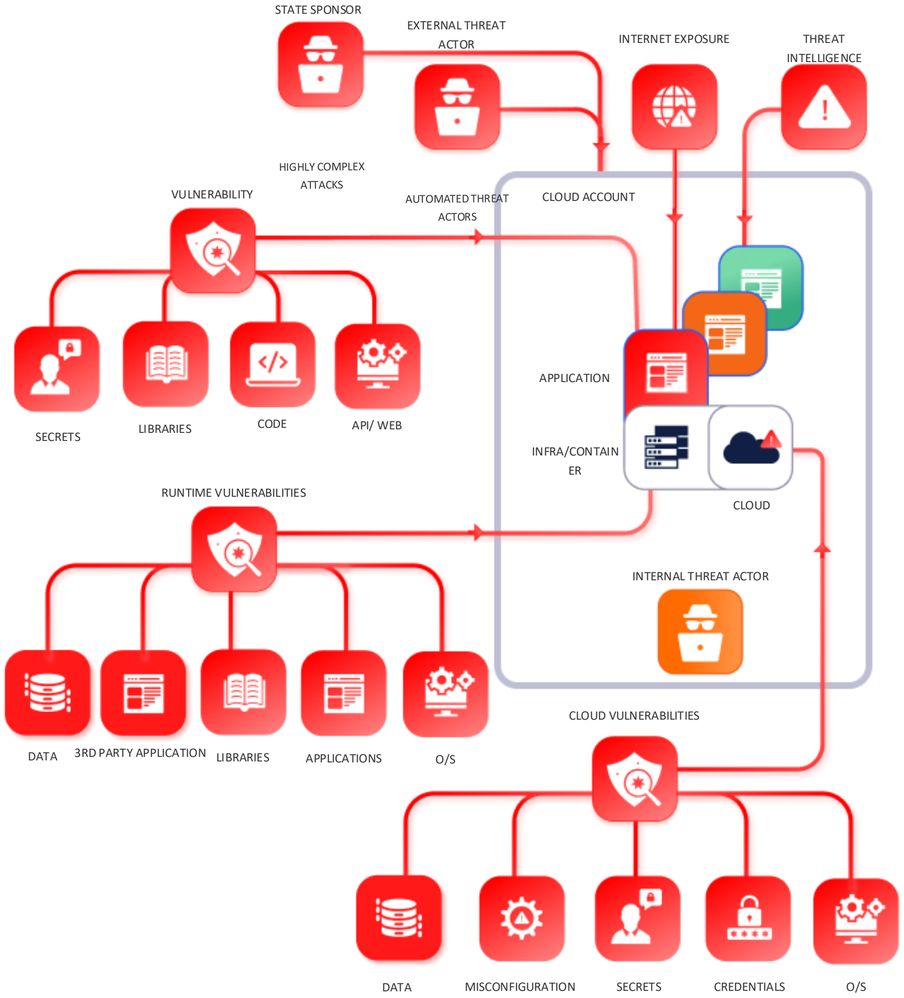
We don’t believe you. Let’s see if you still think so by the end.

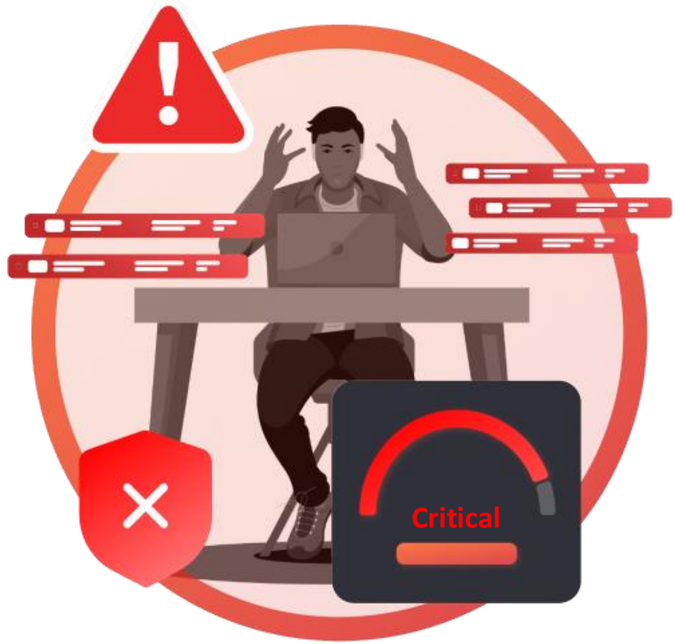
Context: In 2015 we had fewer security tools, digital software supply chain was simpler, and the attack surface was smaller, so finding fixes was trivial



- Total Number of CVEs: 15 K (now 222 K+)
- Few scanners / limited attack surface
- Monolithic software deployed on premises

Context: Today it's becoming impossible to manually find which vulnerability to fix next … when vulnerabilities are getting exploited in 3 minutes





- **Total Number of CVEs Increasing exponentially:**
  280 K (vs 6.7k in 2015)
  40K vuln last year
- **Multiple alerts all disconnected, multiple disjointed processes and reports**
- **Larger software attack surface built by multiple teams releasing frequently**

I feel your pain

Alert FATIGUE

No COMMON LANGUAGE

=

BURNOUT

Vulnerability growth outpaces the ability of defender to react. Automation is the only solution

2025 CVE/FIRST VulnCon

 # CVE

220 538 **

35% YoY increase

Most Vulnerabilities are Critical - High (58%)**

Only 1-10%

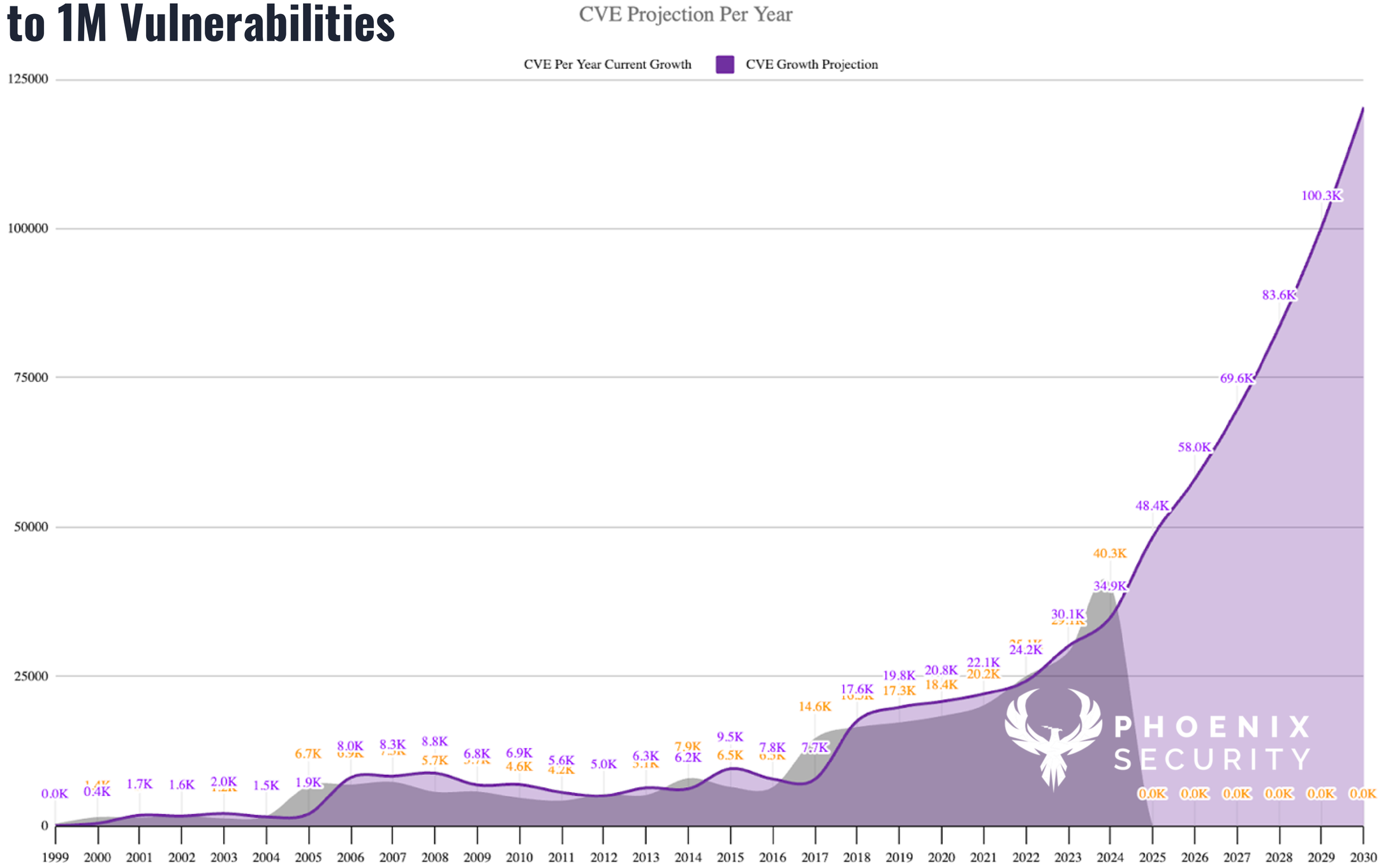
of these is actually relevant *

Only 6%

Budget increase for security team down from 17% ***

*FIST / EPSS ** NVD/CVE STATISTICS *** UK GOVERNMENT

Road to 1M Vulnerabilities



Market – More code than ever, malicious code generator accelerate exploitation time to 3 minutes

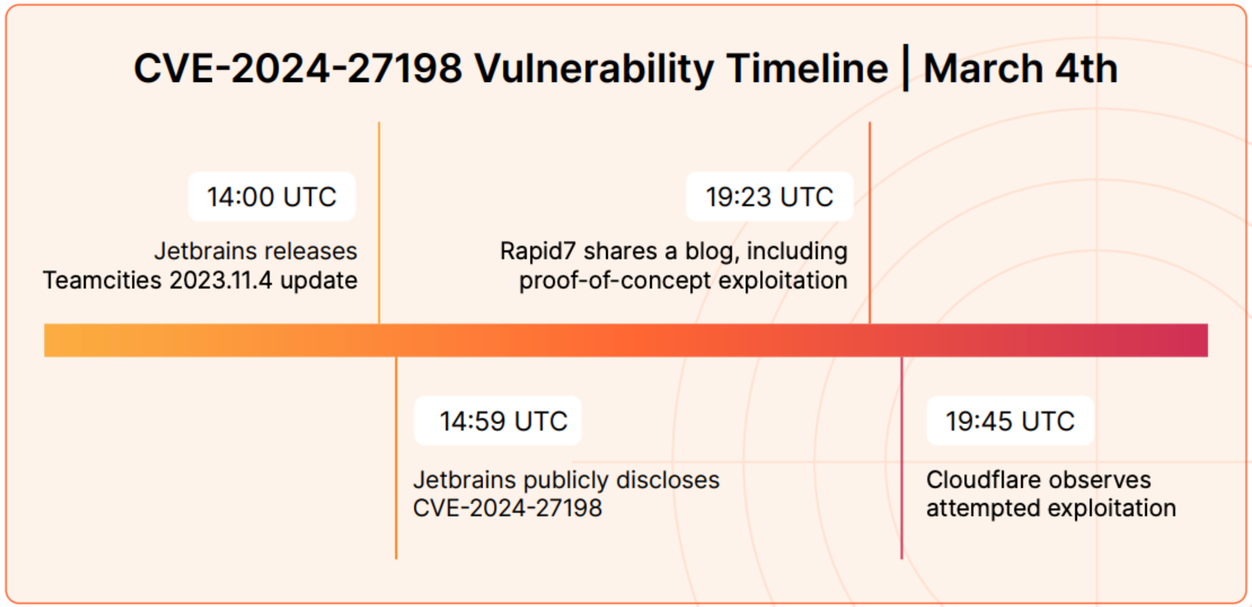
> Data from GitHub reveals that "41% of all code right now is AI generated," Mostaque remarked. More interestingly,
>
> GitHub CTO

State of Malicious underground LLM to develop malicious code*

Table 1: *Malla* services and details

Name	Price	Functionality			w/wo voucher copy	Infrastructure
		Malicious code	Phishing email	Scam site		
CodeGPT [11]	10 βytes*	●	○	◐	No	Jailbreak prompts
MakerGPT [49]	10 βytes*	●	○	◐	No	Jailbreak prompts
FraudGPT [30]	€90/month	●	●	●	No	-
WormGPT [79, 80, 83]	€109/month	●	●	◐	No	-
XXXGPT [28, 61, 84]	$90/month	●	○	○	Yes	Jailbreak prompts
WolfGPT [77, 78]	$150	●	●	●	No	Uncensored LLM
Evil-GPT [26]	$10	●	●	●	No	Uncensored LLM
DarkBERT [16, 17]	$90/month	●	●	○	No	-
DarkBARD [14, 15]	$80/month	◐	◐	○	No	-
BadGPT [2, 3]	$120/month	◐	◐	◐	No	Censored LLM
BLACKHATGPT [4–6]	$199/month	●	○	○	No	-
EscapeGPT [23]	$64.98/month	●	◐	◐	No	Uncensored LLM
FreedomGPT [32, 33]	$10/100 messages	●	◐	◐	Yes	Uncensored LLM
DarkGPT [18, 19]	$0.78/50 messages	●	◐	◐	Yes	Uncensored LLM

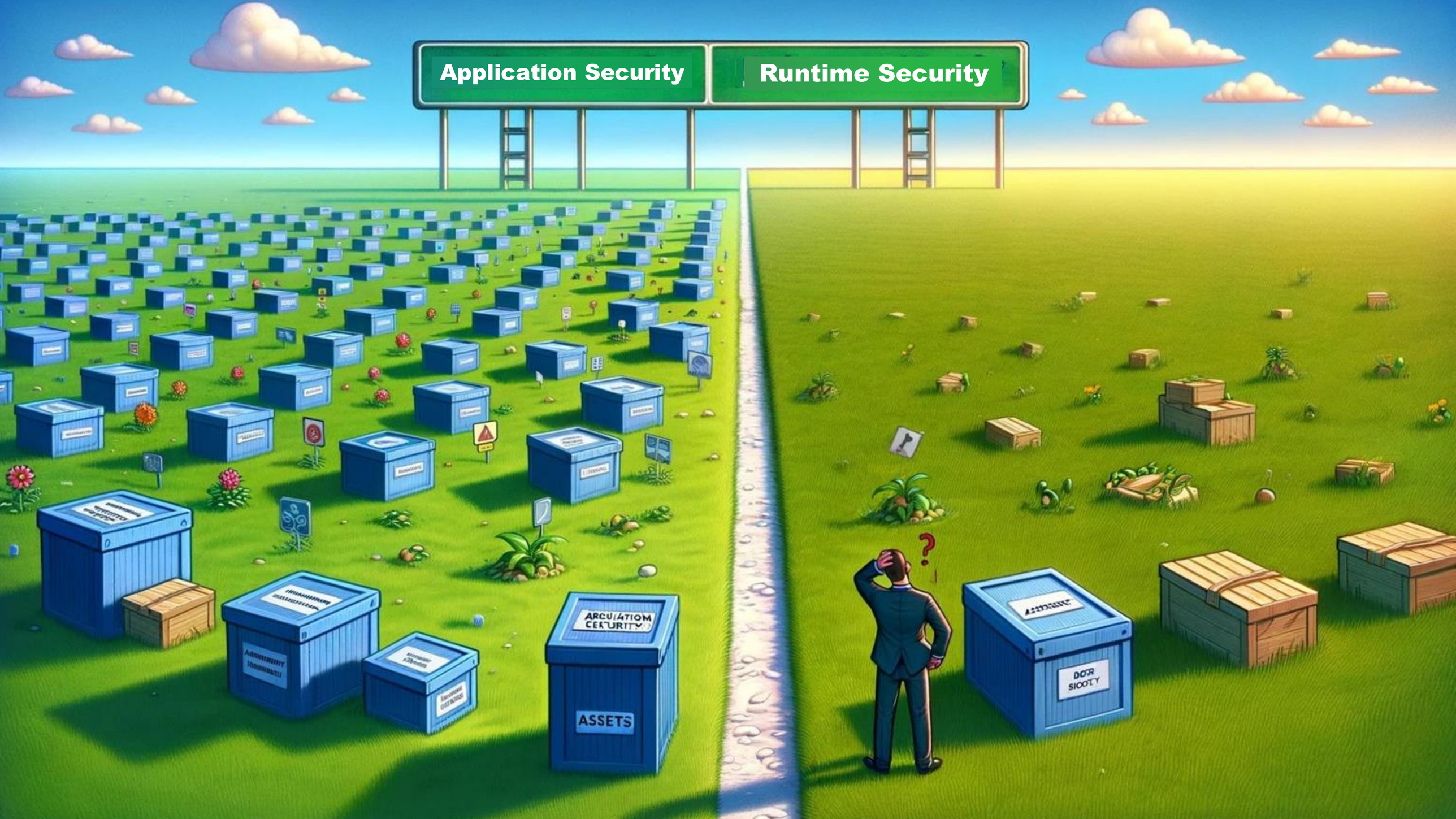
* βytes is the forum token of `hackforums.net`; ◐ indicates implicit mention.

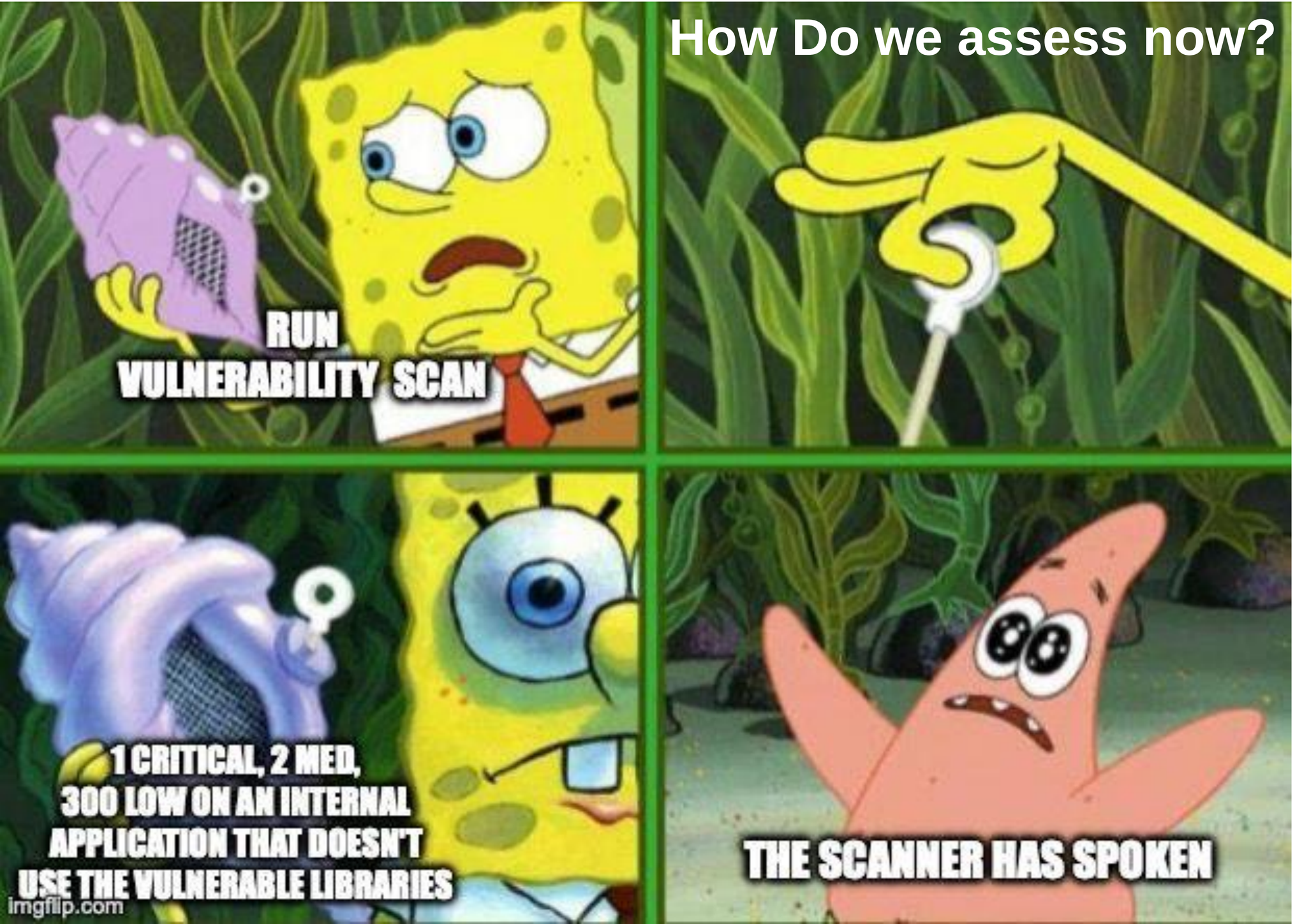


← 3 Minutes** →

*https://arxiv.org/abs/2401.03315

**https://blog.cloudflare.com/application-security-report-2024-update/


Application Security
Runtime Security
ASSETS


How Do we assess now?
RUN VULNERABILITY SCAN
1 CRITICAL, 2 MED, 300 LOW ON AN INTERNAL APPLICATION THAT DOESN'T USE THE VULNERABLE LIBRARIES
THE SCANNER HAS SPOKEN
imgflip.com

The Vulnerability Cycle

Step 1 – Overload Dev

Step 2 – Pray they catch that 1 vulnerability

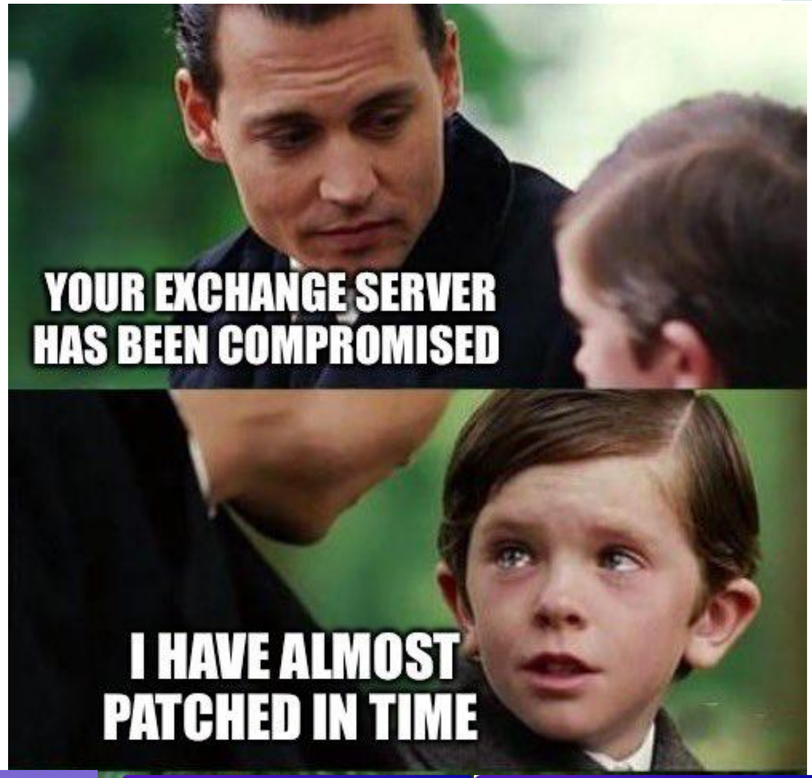
Step 3 – That 1 vulnerability get compromised

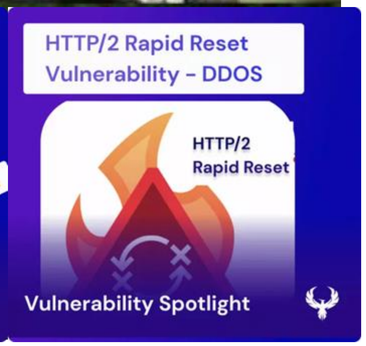
Step 4 – Shocked Executive, we asked security to be secure

Step 5 – Overload Team some more with latest buzzword scanner

Bonus – Executive mention do security > Security replies fix with SLA

How do we address this problem





The question we try to answer NOW

HOW MANY problems have we addressed and how quickly

Questions we should be answering

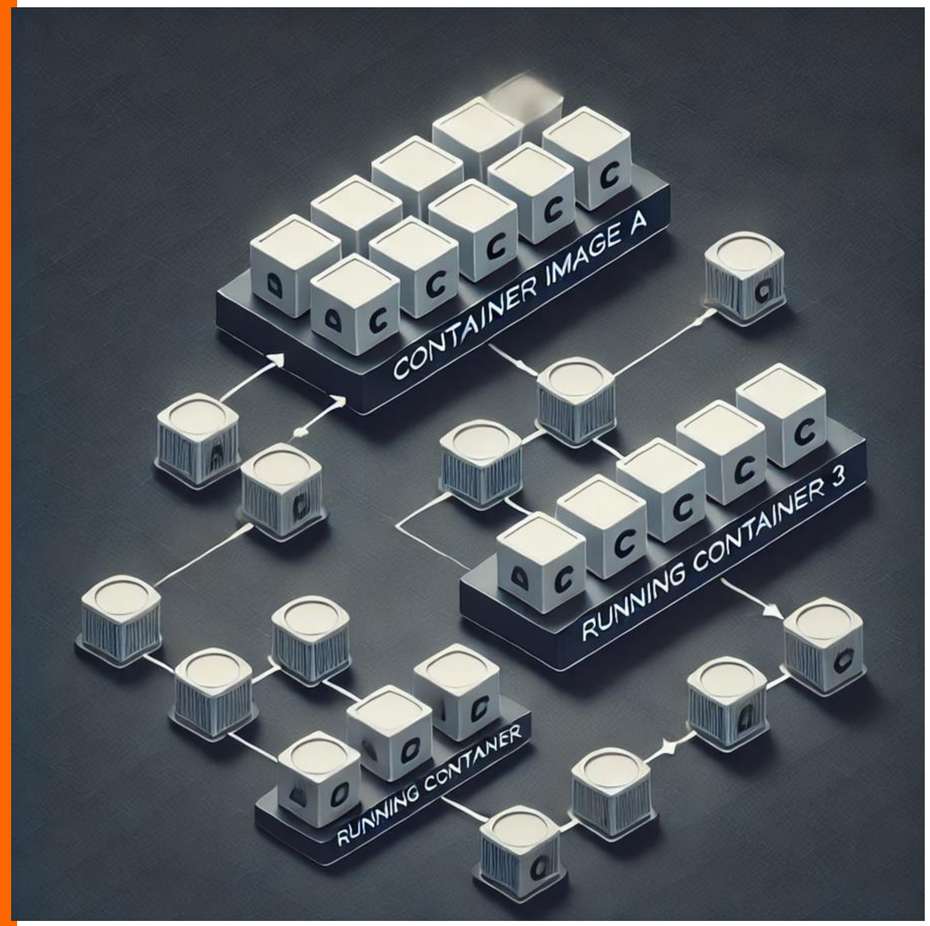
WHO does WHAT where and how IMPORTANT is it

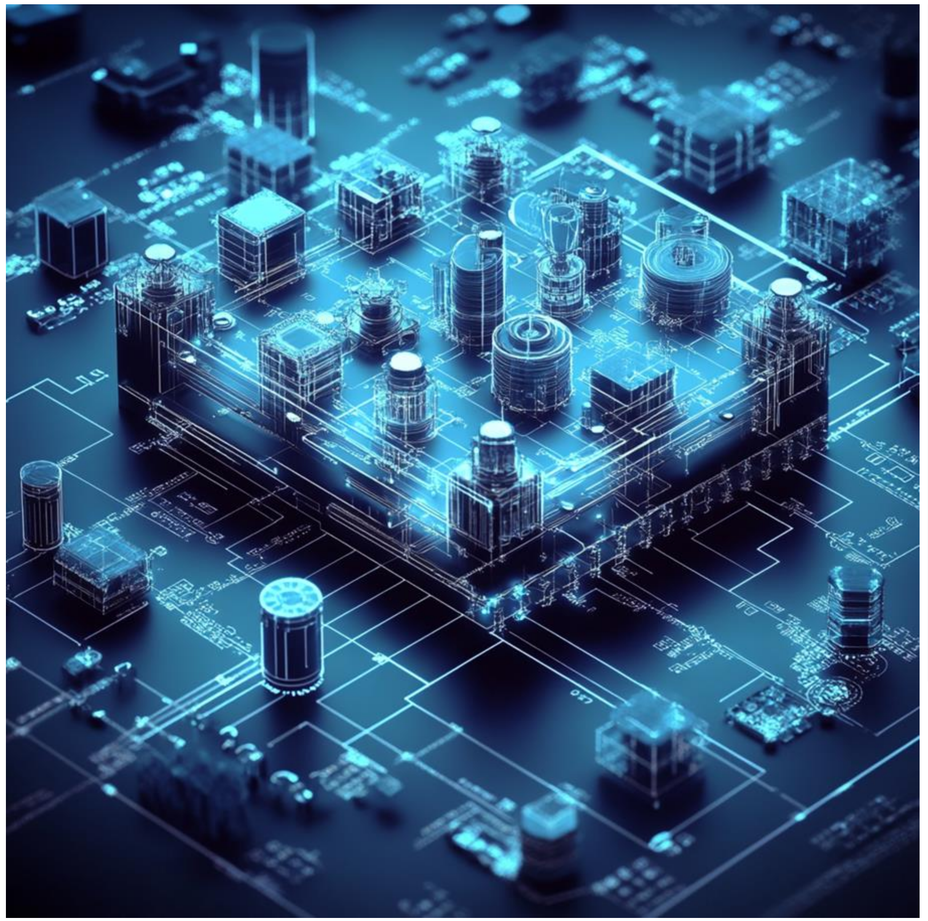
But really… is it reachable

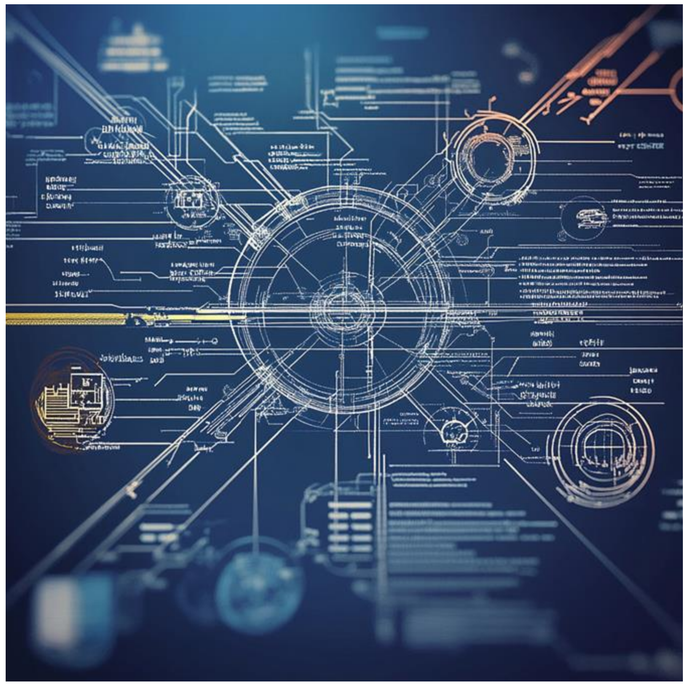
Part 1 - The Rant

"building the picture" - but doing it wrong

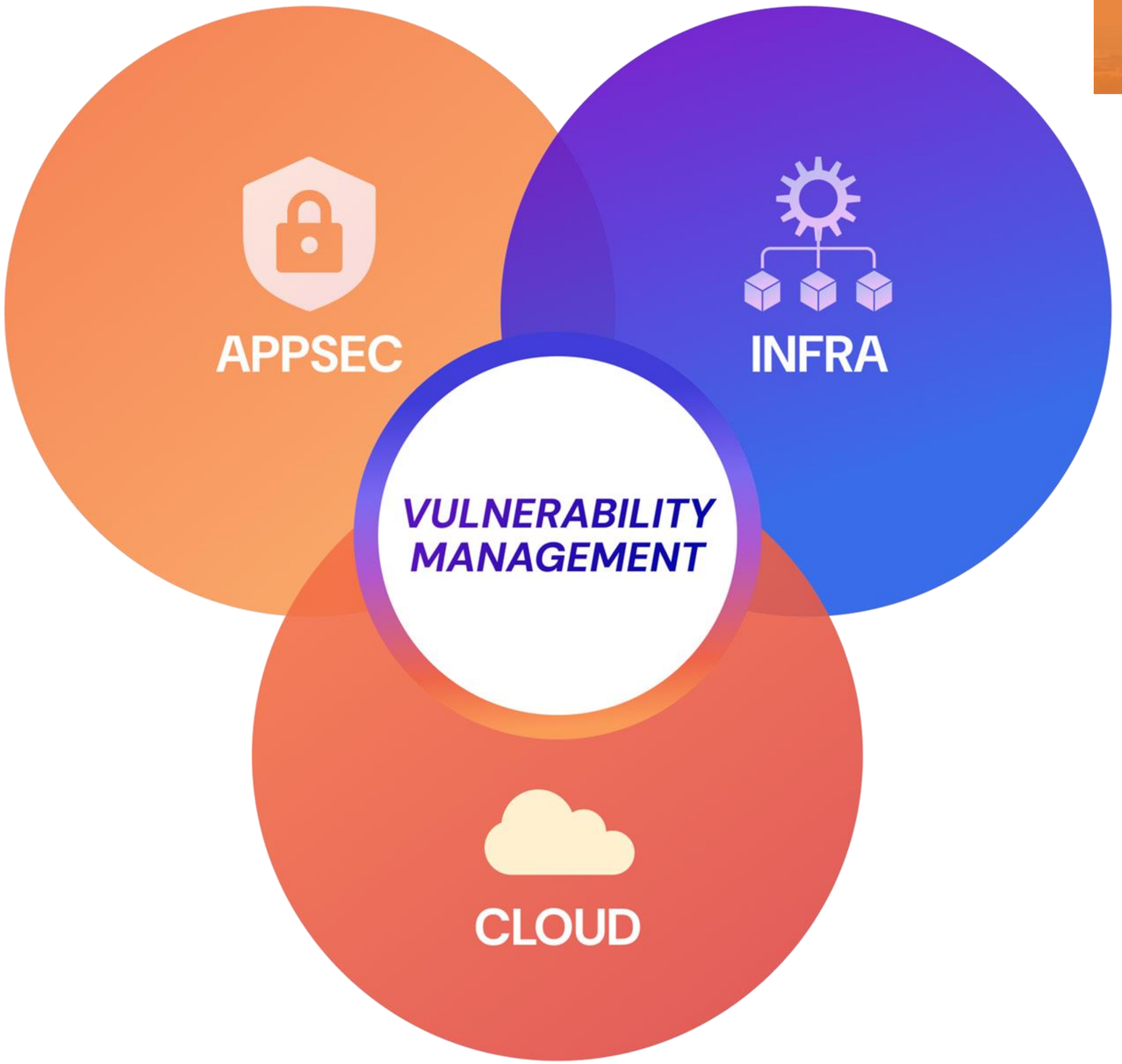
context is king







AppSec, Infra, Cloud, etc., are all part of the same Vuln Management Exercise



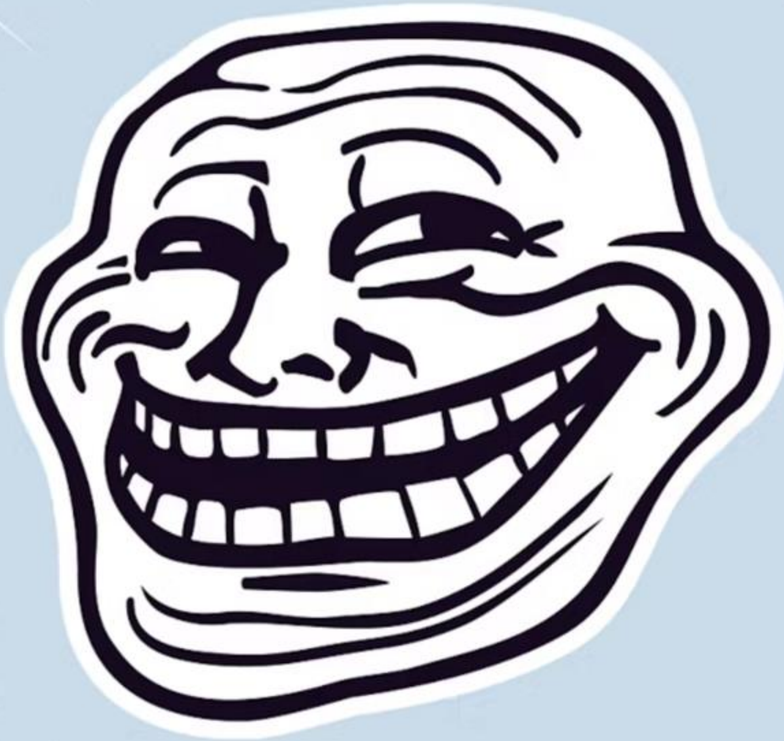
Build vs. Buy is it still applicable?

But I’m here to give you the silver bullet

2025 CVE/FIRST VulnCon

THE QUICK FIX!

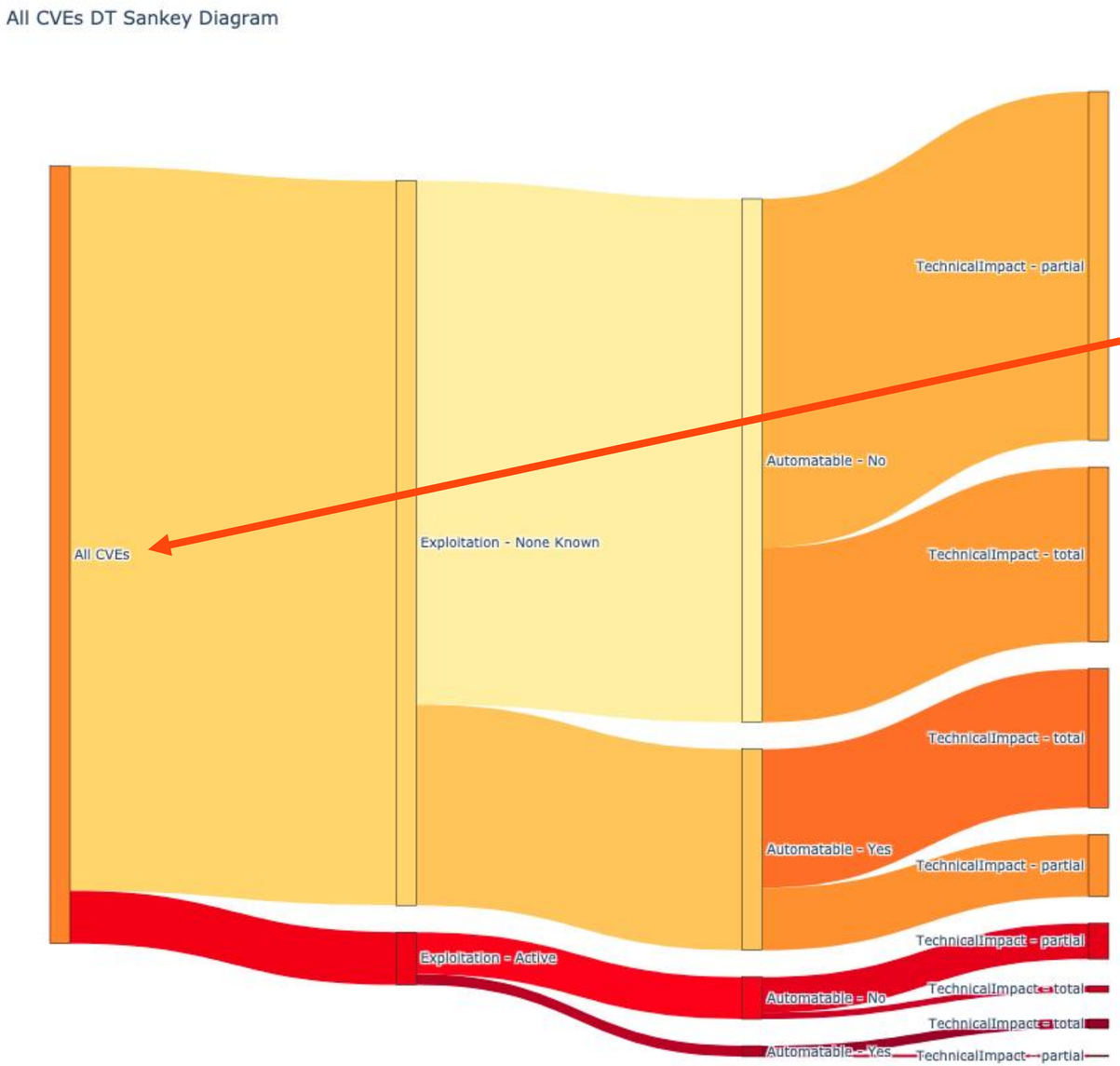
What quick fix?



What is a VM program

Part 1 – Frank Identify what to fix first IS COMPLEX

Current Flow of vulnerabilities only 1% are exploitable



Current Focus

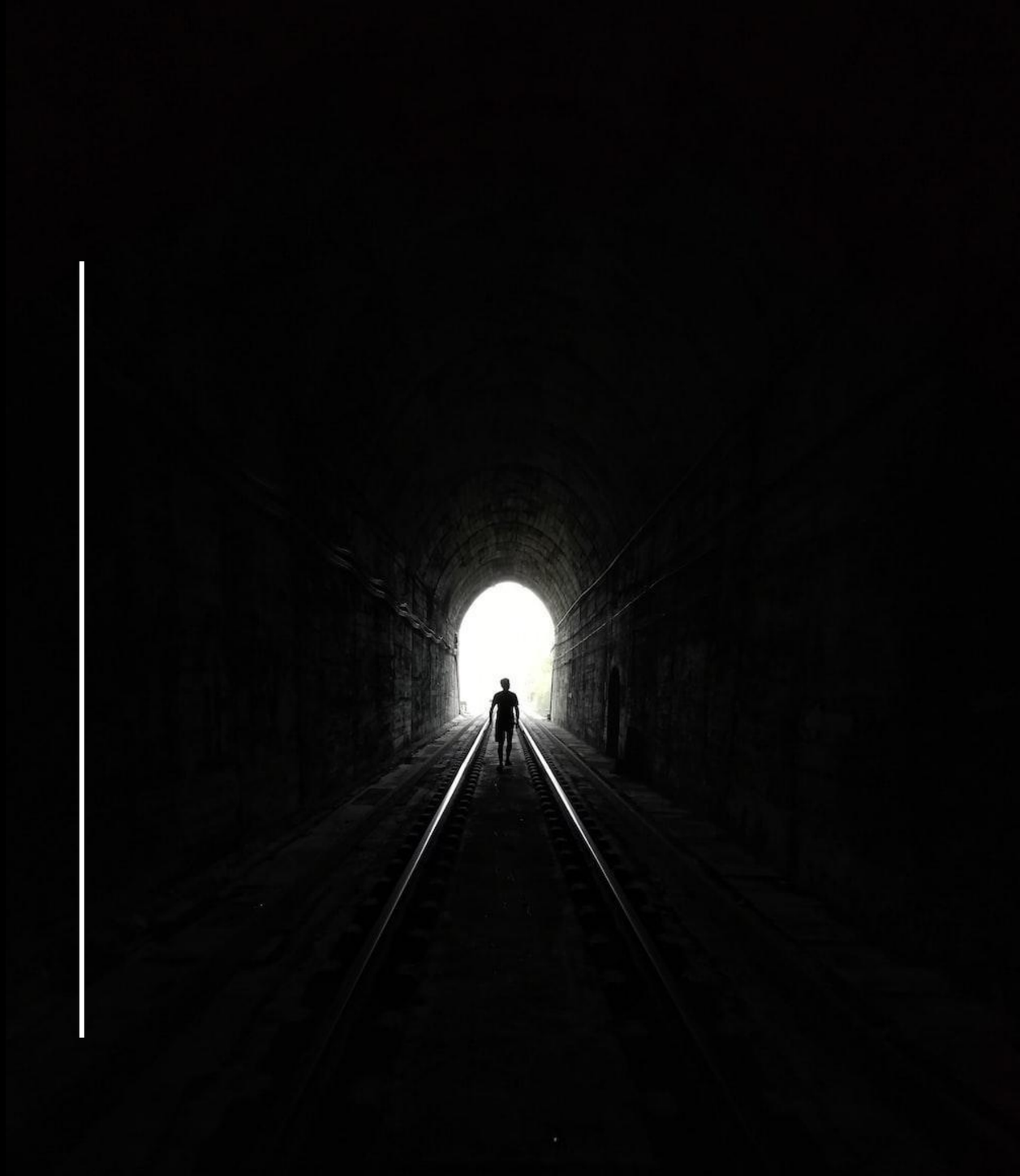
Really important to focus on

* Credit Chris Madden

All Doom and gloom?

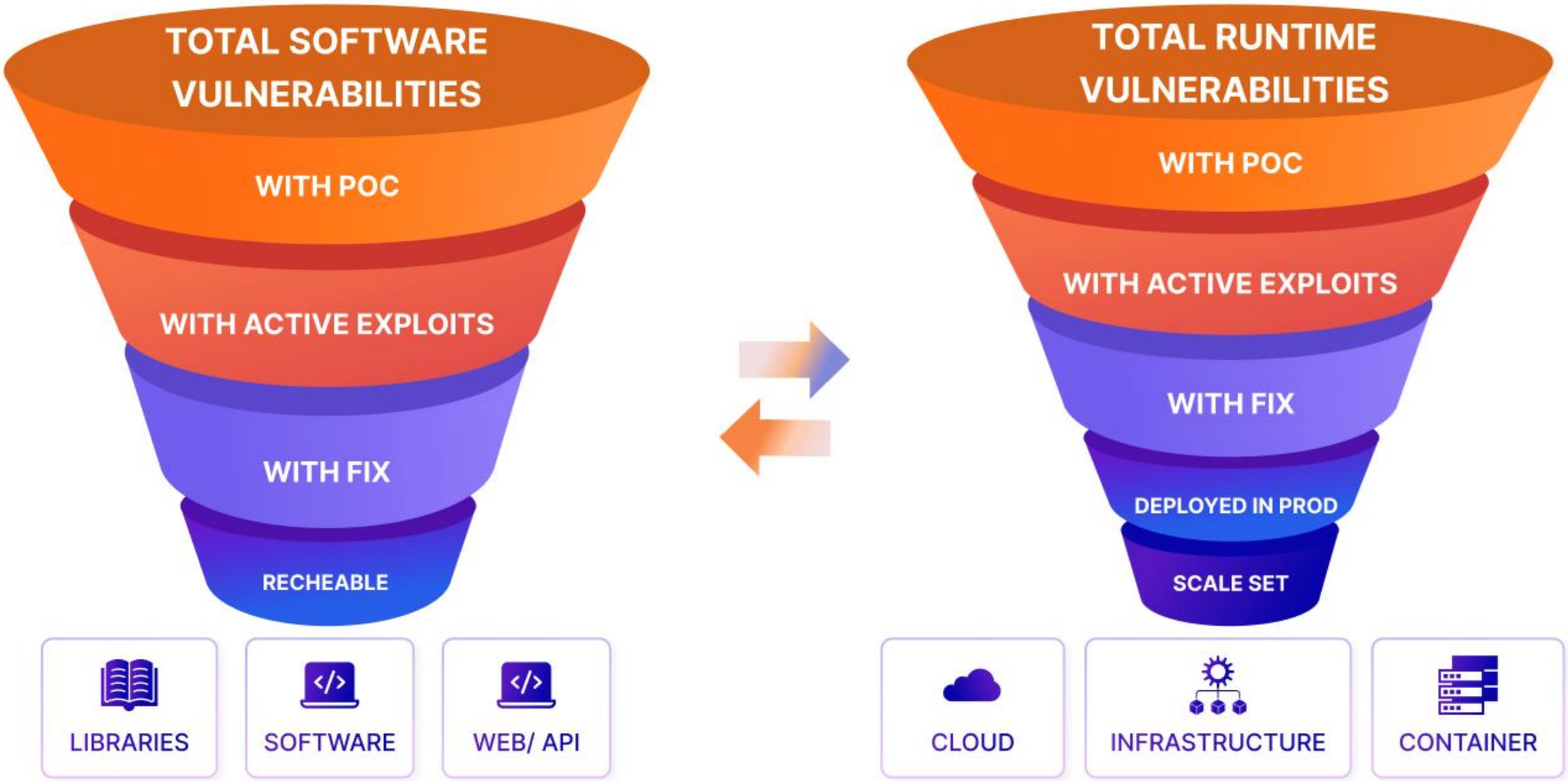
There is a light at the end of the tunnel

- Vulnerability ARE NOT fixed on risk objectives
- Vulnerabilities ARE NOT Prioritized or contextualized
- Vulnerabilities ARE NOT Attributed to the right team
- Asset inventory still a myth, are you aware what software runs in your pipeline

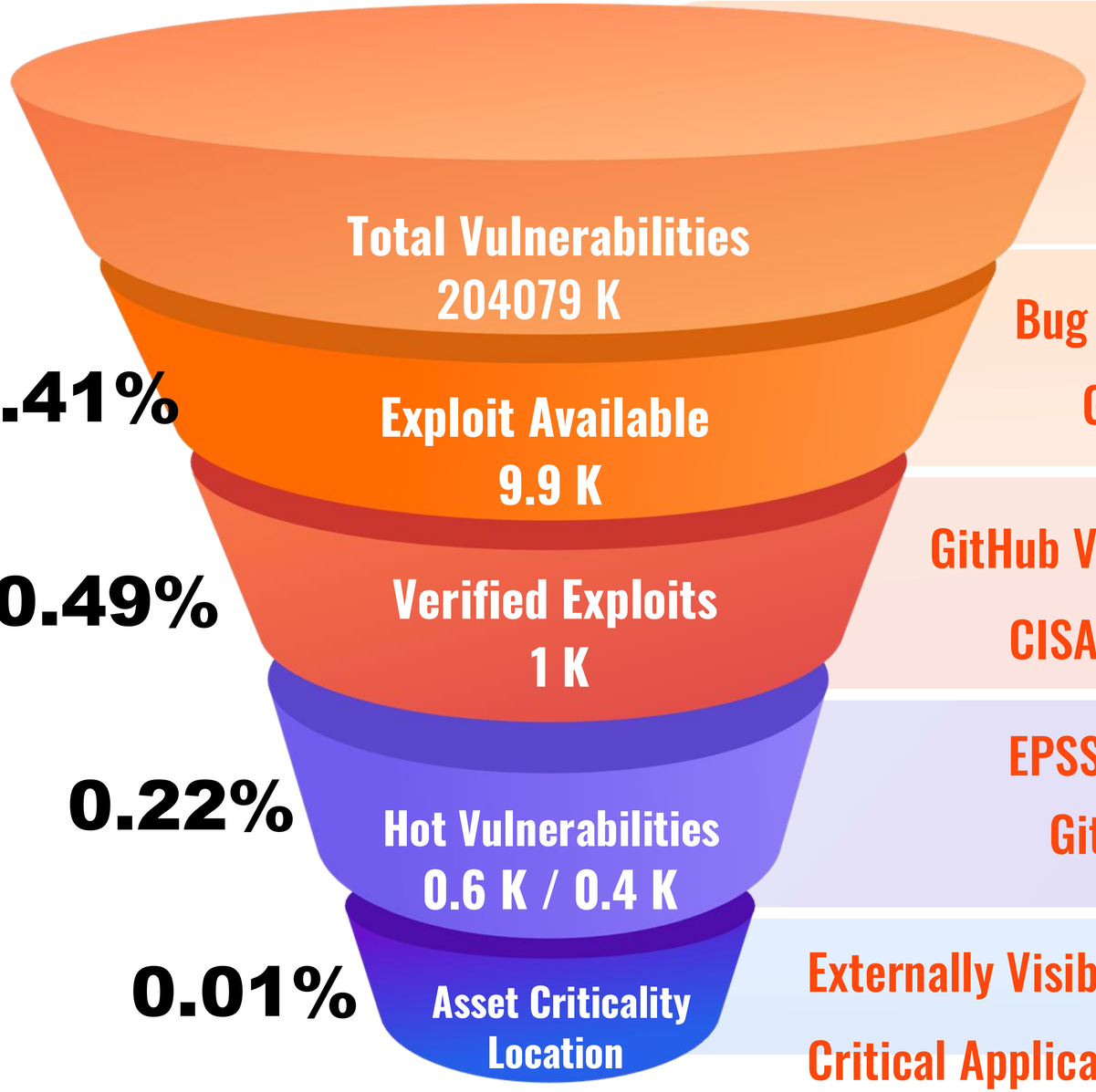


Attributing the right vulnerability with right context

Common Root Cause



Not all the vulnerabilities require equal attention



Bug Bounty Popularity (active 17K) 8.33%

GitHub Exploit (9.9K) 4.41%

GitHub Verified Exploits (0.93K) 0.47%

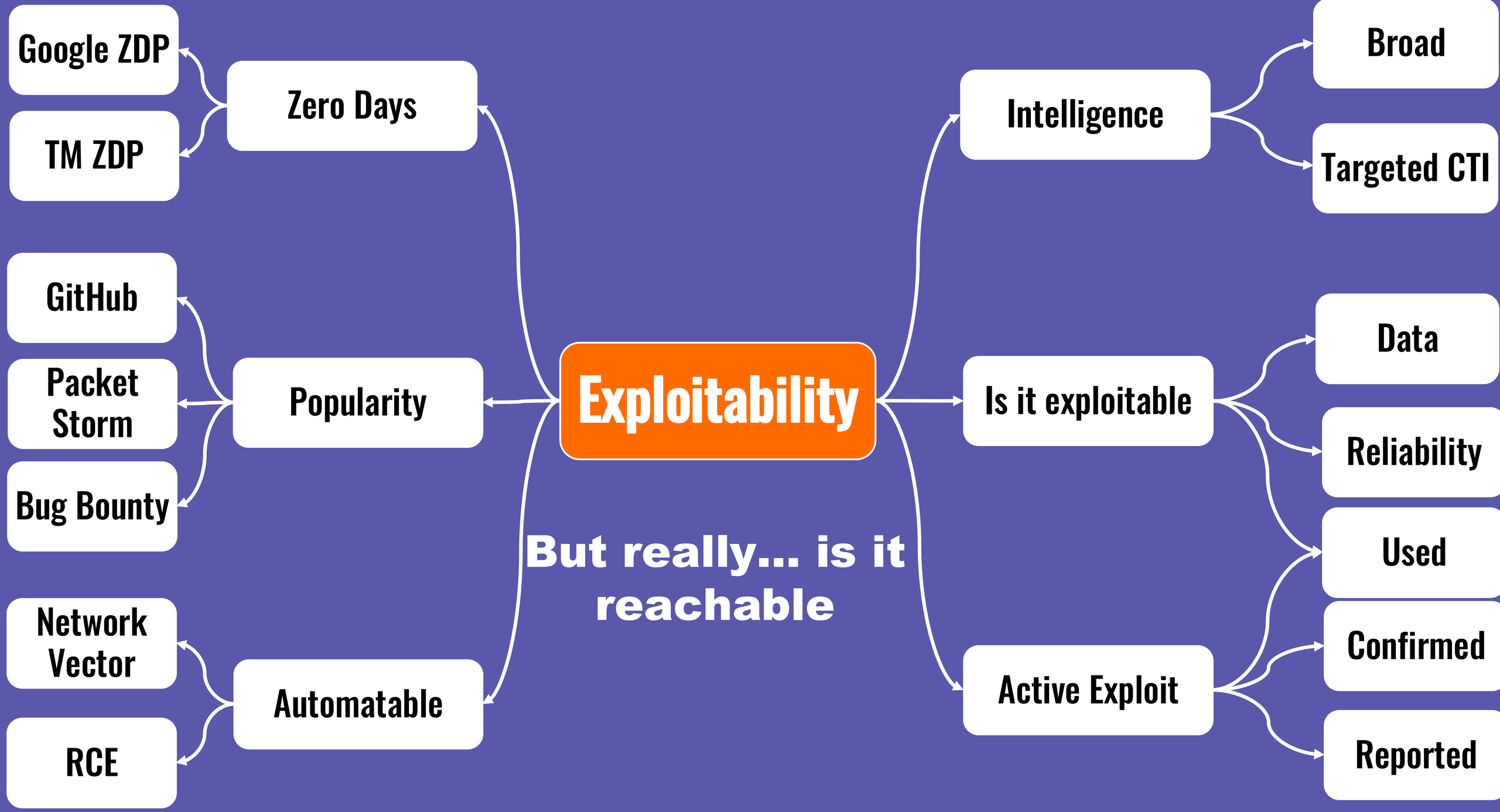
CISA KEV (1K) 0.49%

EPSS > 0.7 (688) 0.34%

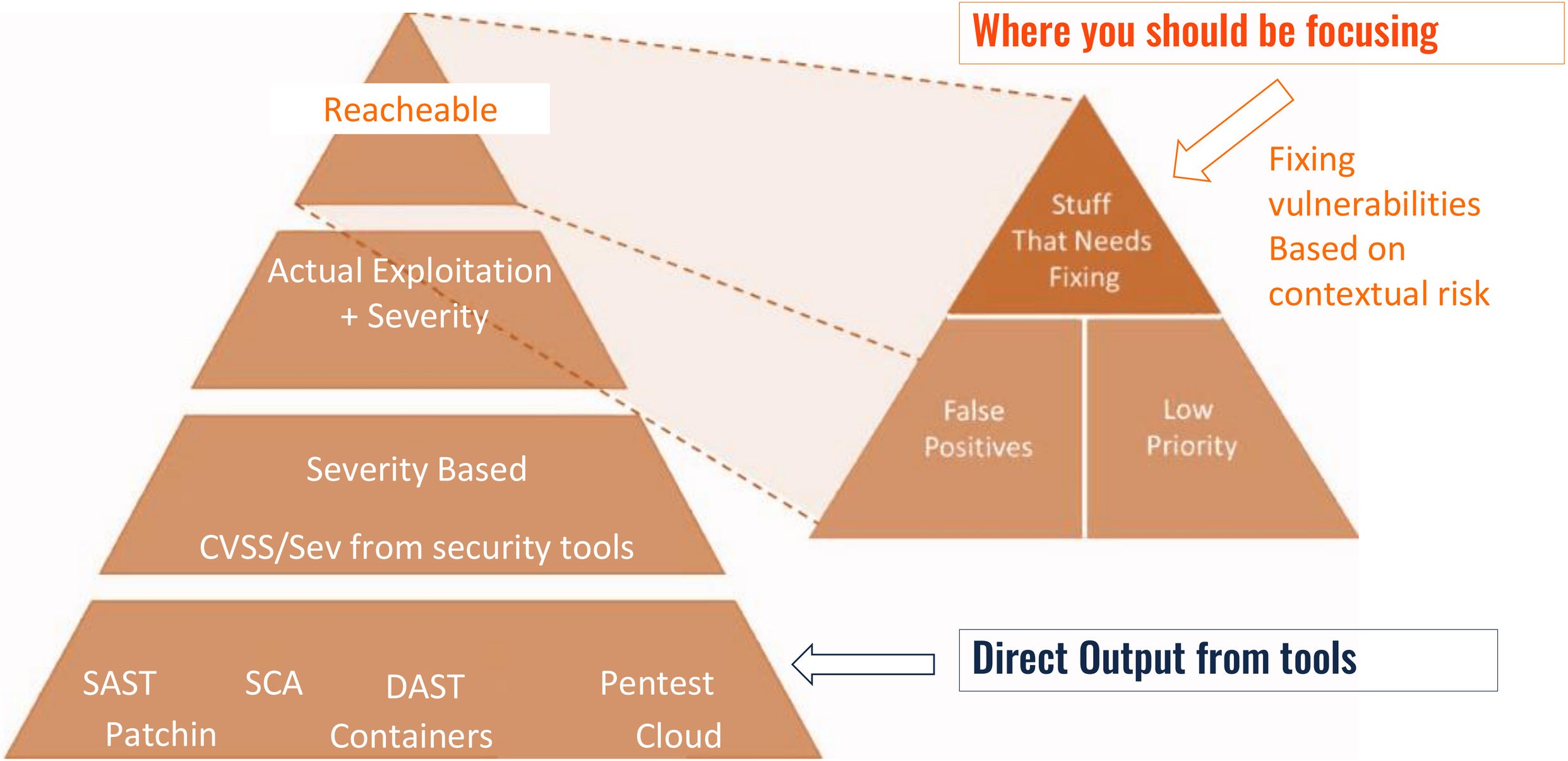
GitHub Active Exploit (0.40K) 0.22%

Externally Visible (0.14) ? 0.?%

Critical Application

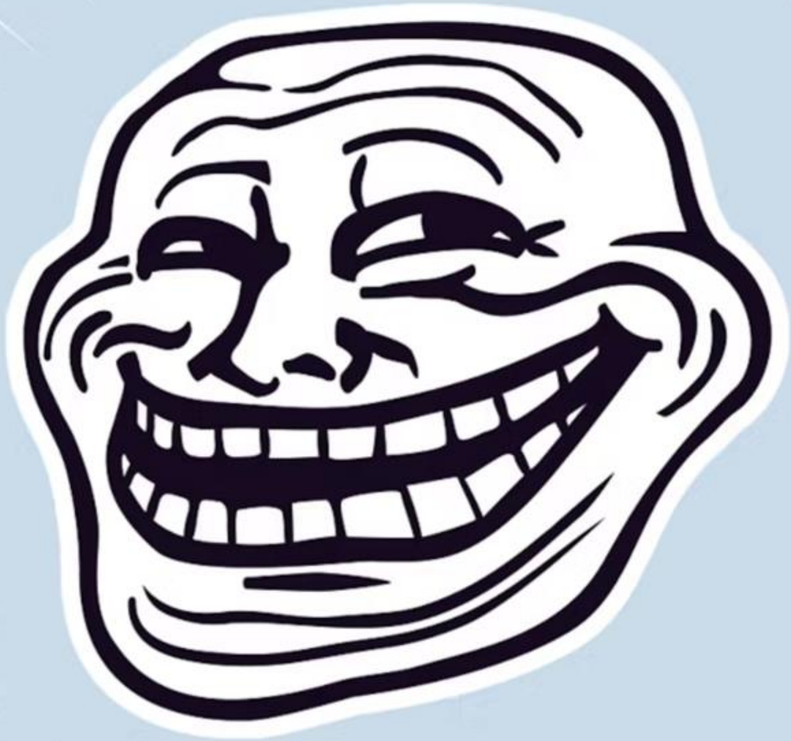

Google ZDP
TM ZDP
Zero Days
GitHub
Packet Storm
Bug Bounty
Popularity
Network Vector
RCE
Automatable
Exploitability
But really... is it reachable
Intelligence
Broad
Targeted CTI
Is it exploitable
Data
Reliability
Active Exploit
Used
Confirmed
Reported

Prioritization is so 90....

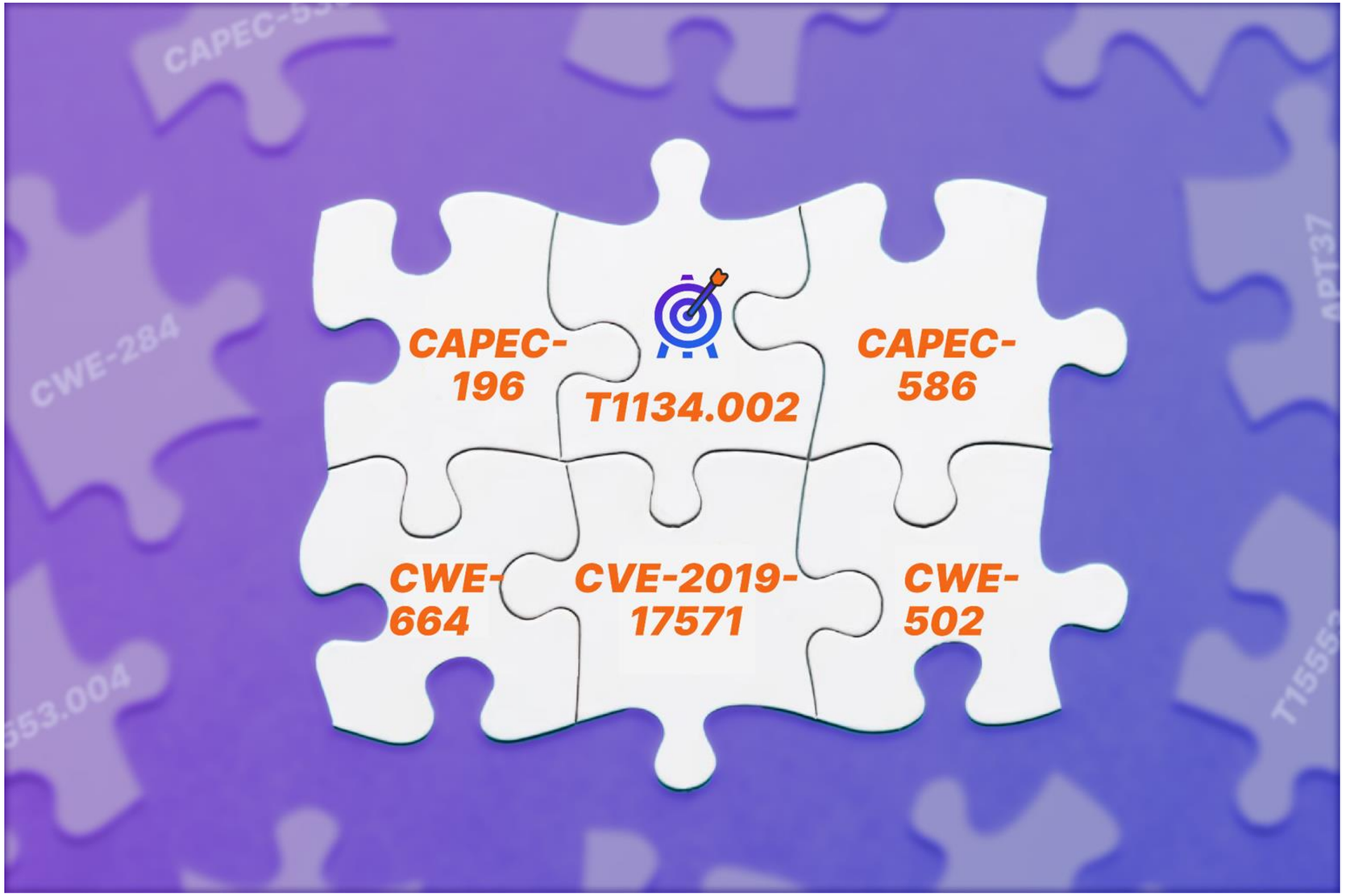


Part 2 - Nate - The silver bullet(s)

What quick fix?



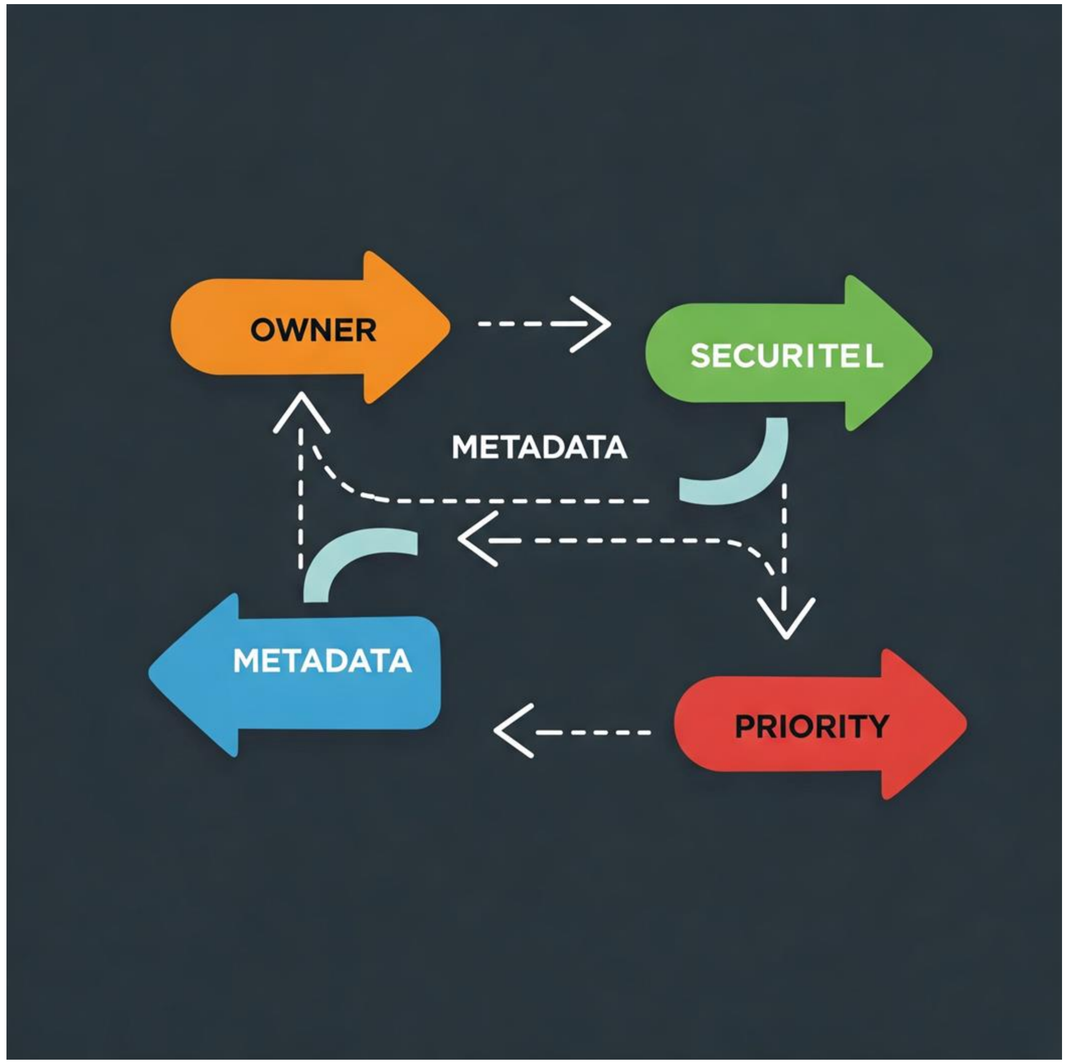
From Chaotic Data, unclassified and just a list of vuln to organized data

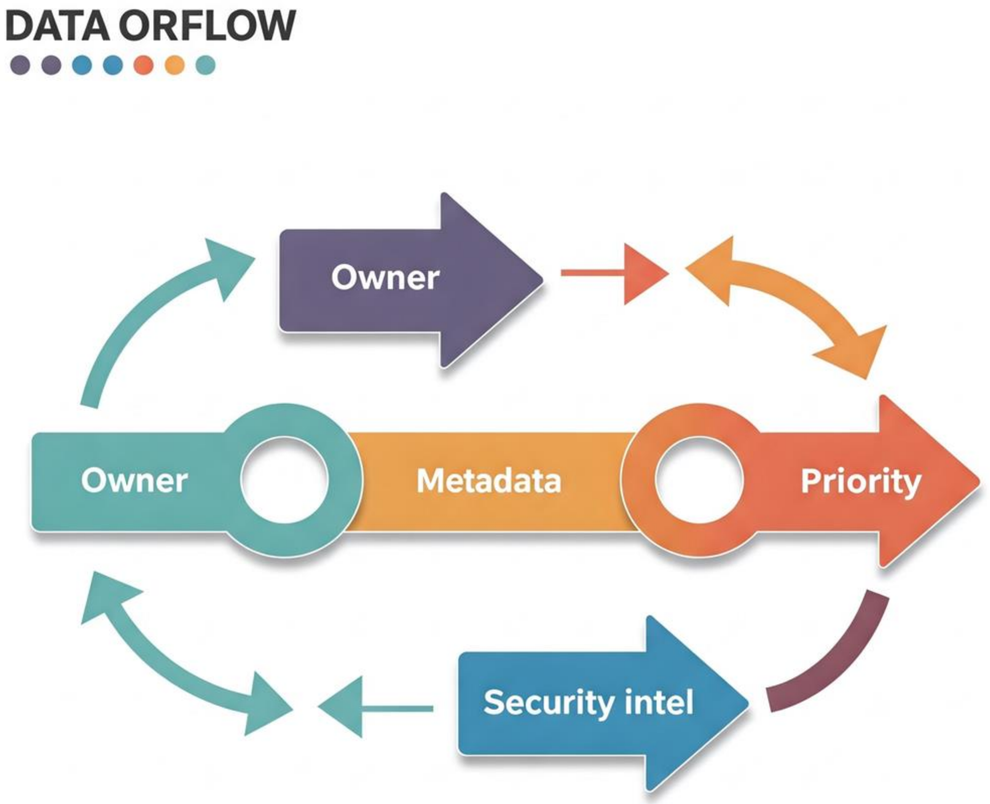


Asset Ownership the foundation

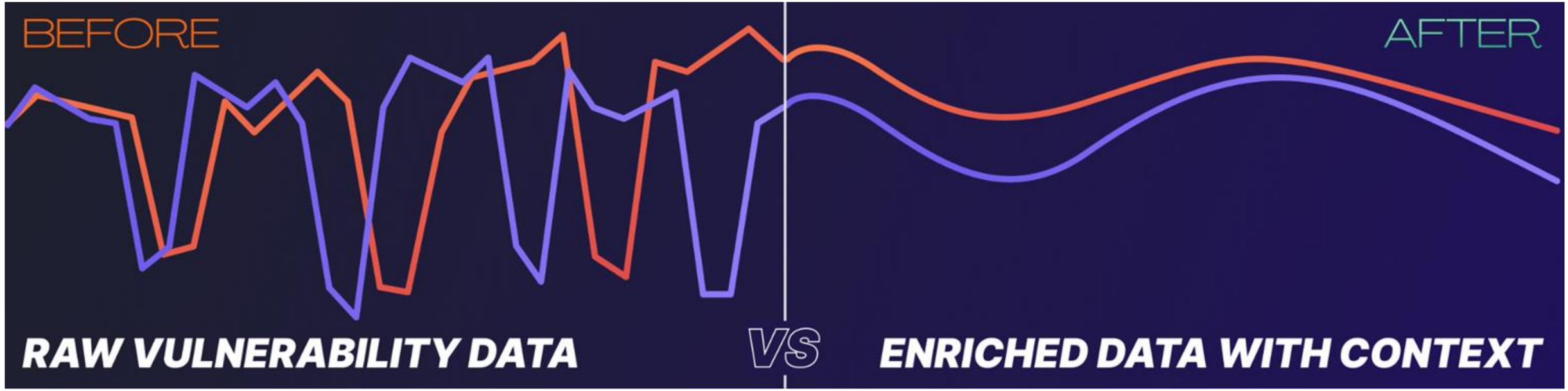
From Uncontextualized and chaotic data to Precise Backlogs

Who needs to do what and how we identify the owners





raw vuln data vs. enriched data with context.

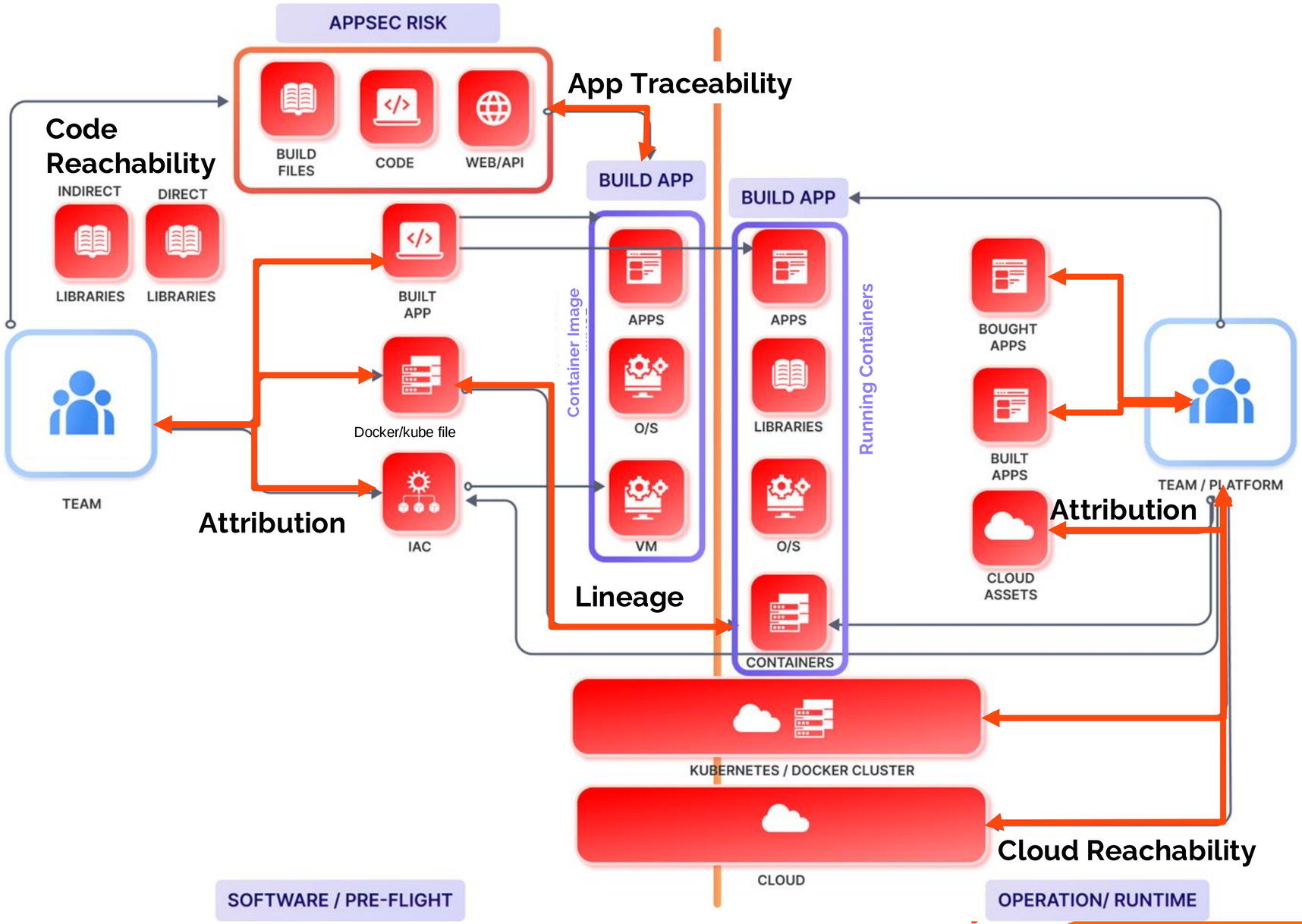


But most important: Who owns it, is it important, when does it need to be fixed

Part 2 - Connecting the dots, Code and Cloud

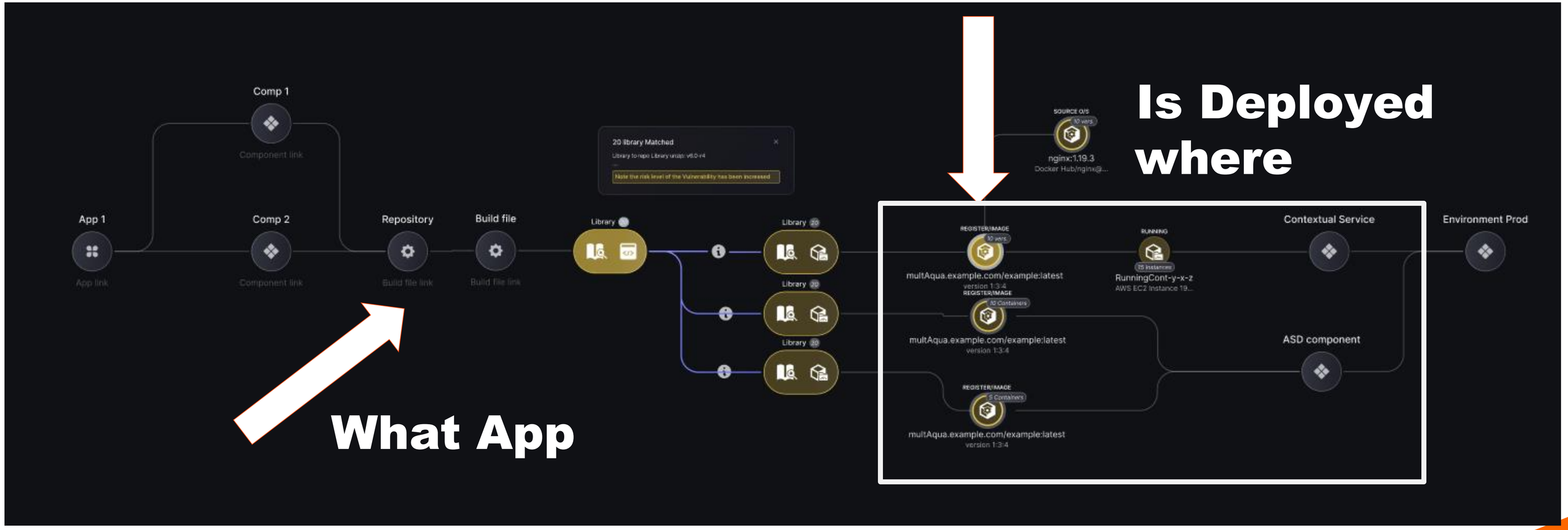
Phoenix correlates, contextualizes and deduplicates by linking together assets using 4 dimensions

- Attribution
- Lineage
- Traceability
- Code/Cloud Reachability



An example of complexity Container fixing :

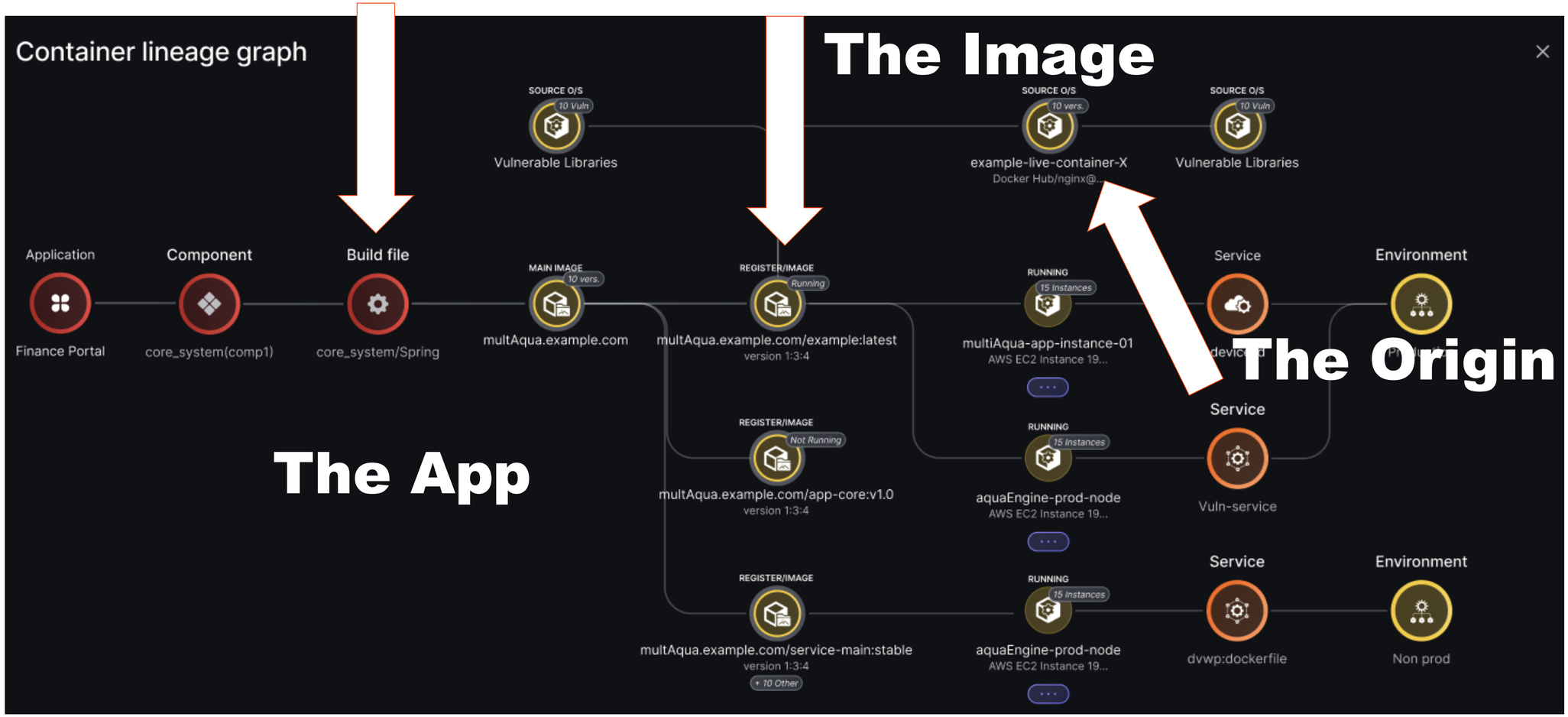
Libraries that are deployed : fix in the library vs fix in containers



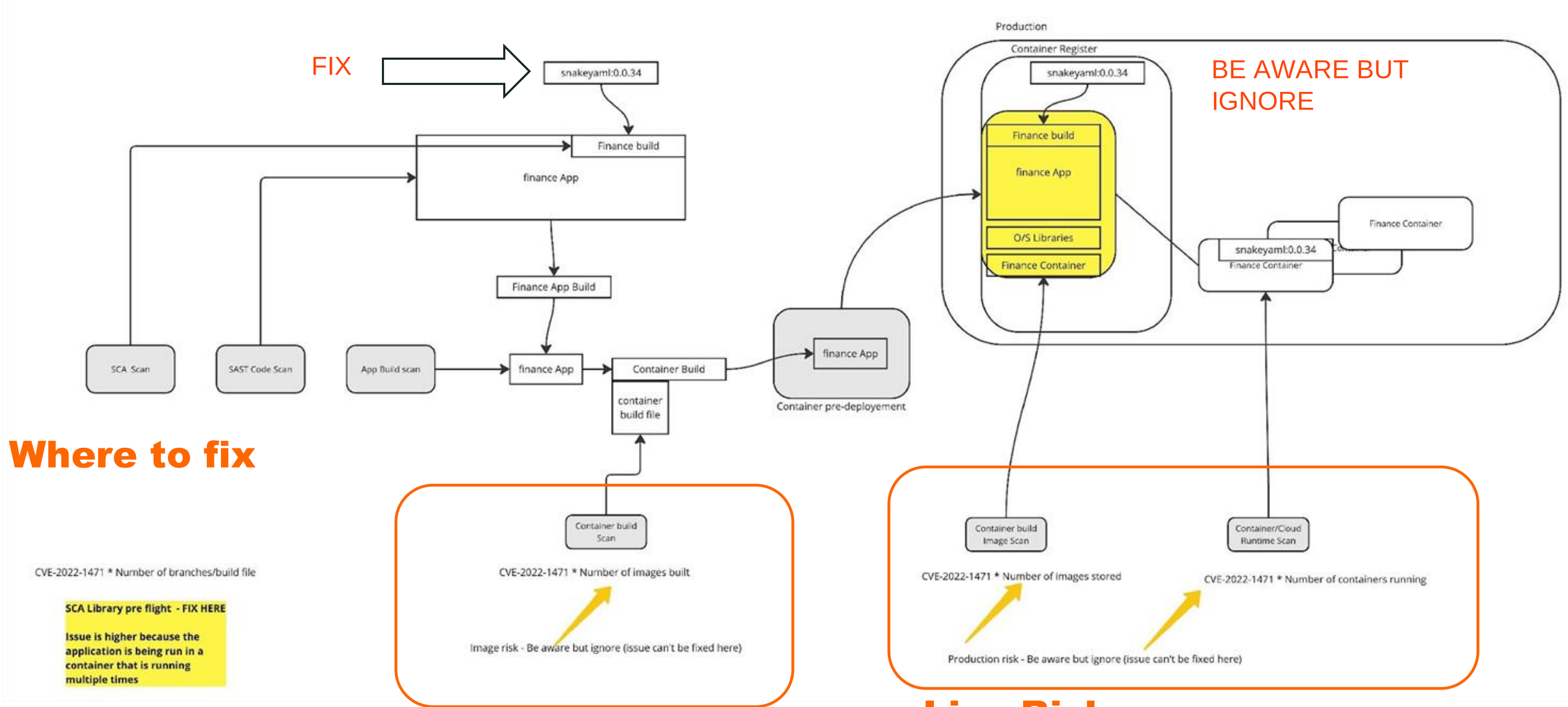
Container Deployment Lineage – What to fix where?

Why trying to patch all containers when

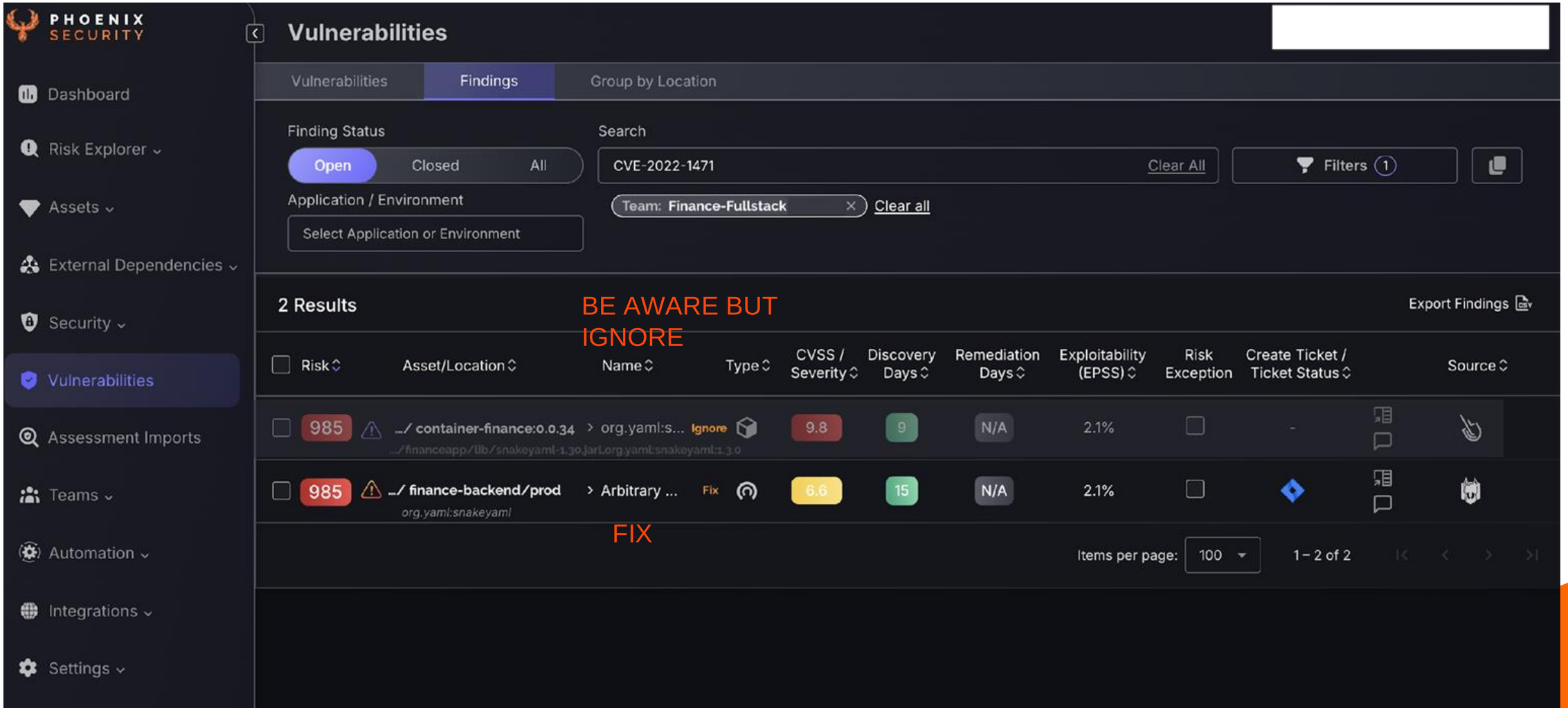
- Libraries to patch needs to be fixed by dev team
- Container images needs to be solved at root
- Sometimes the problem is with source containers



Real Case Scenario : Deduplicating Contextually Code and Libraries



Real Case Scenario : Deduplicating Contextually Code and Libraries



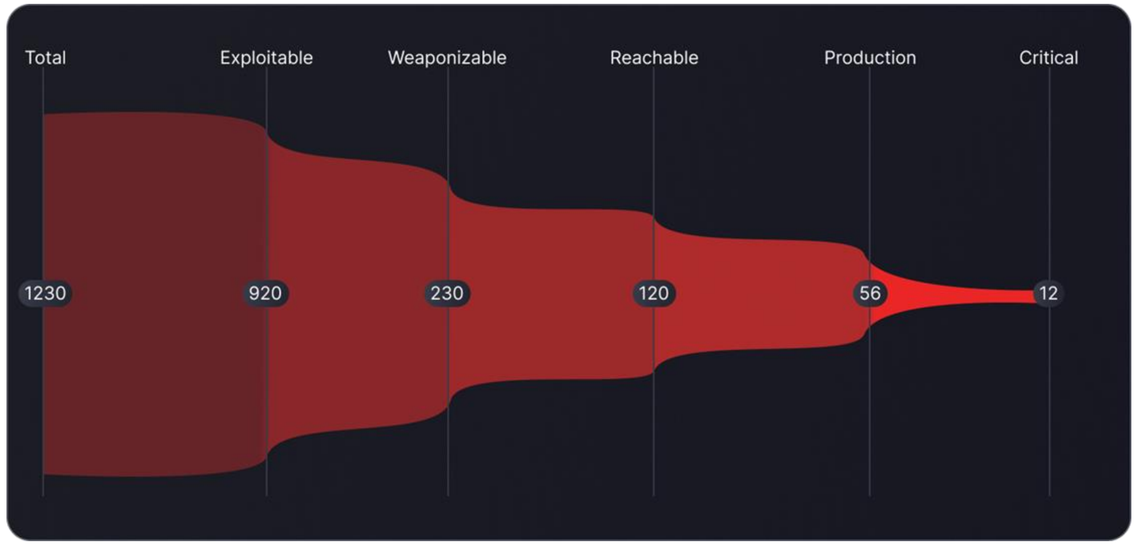
Reachability Analysis of a Vulnerability

	1 Code Reach Analysis	2 Runtime Reach Analysis	2 Container Reach Analysis	4 Network Reach Analysis	3 CTI	3 CTI - Exploitability
WHAT	Analyze function or library being created	Test if library is being loaded in container	Detect if the container is being loaded	Verify if a container's library/node is reachable	Like EPSS identify if a vulnerability is being exploited	Exploit evidence of a vulnerability
WHEN/ WERE	Code, Repo, Build	Runtime/ Build	Cluster analysis of container	Cloud/ Operation	Everywhere	Everywhere
BENEFITS	Reduce vulnerabilities in lib/function not used	Helps identify if the code is being loaded in a container, and which container	Image of the container is being used in runtime	Helps identify if the vulnerability can be reached from Remote	Prioritization of vulnerabilities based on exploitation in wild	Prioritization of vulnerabilities based on exploit evidence
LIMITATIONS	Complex and per language	More intrusive and intensive in some instances Might require Pipeline integration	Requires connection to container	Cloud/ Network reachability analysis	Only works for network detectable Exploits	Base indicator If there is an exploit in the wild

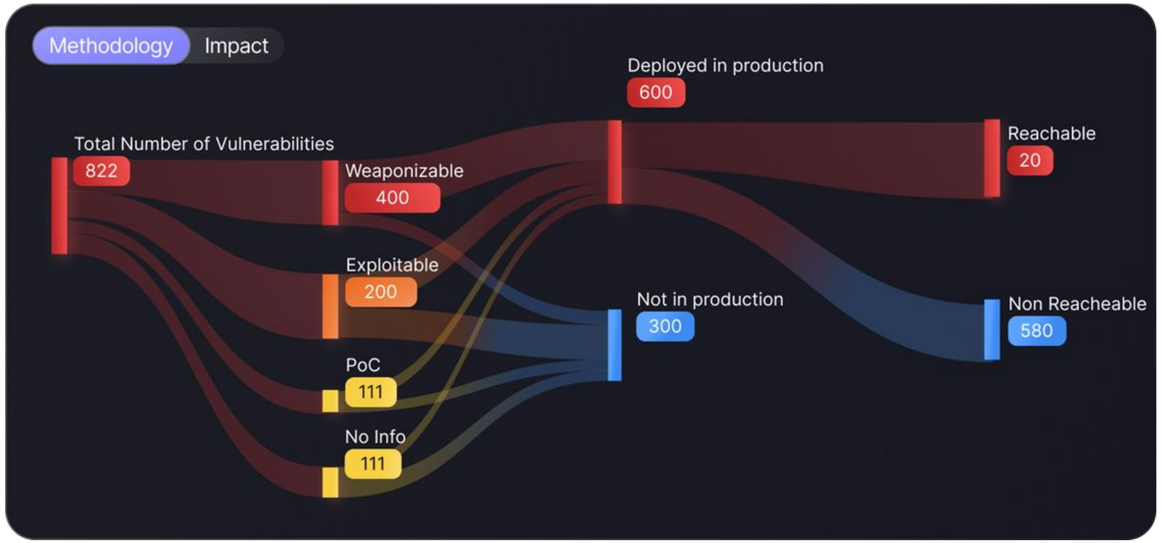
Part 3 – Risk based Approach

THE GOAL - > ANSWERING QUESTION -> AM I EXPOSED?

How many Vulnerabilities are actually important

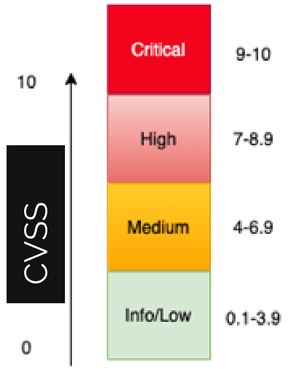


How many exploitable/Weaponizable vulnerability you have

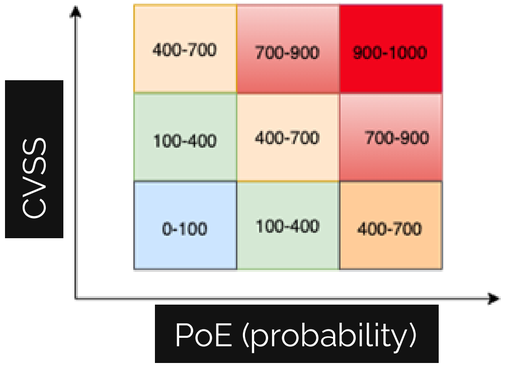


PHOENIX BRINGS OUT THE 4TH DIMENSION OF REACHABILITY

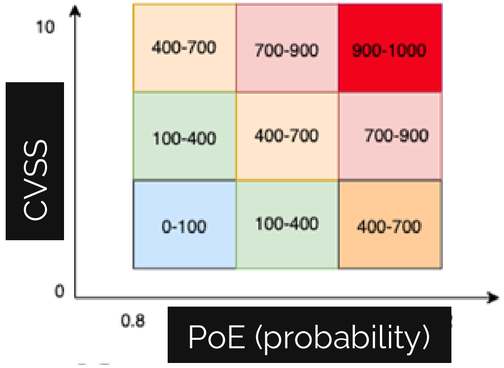
Current Method



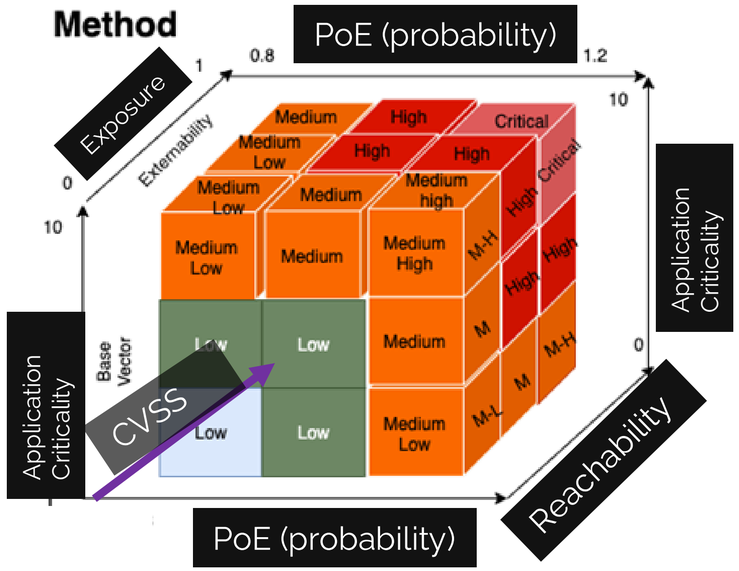
Risk Based Method



Context Based Method



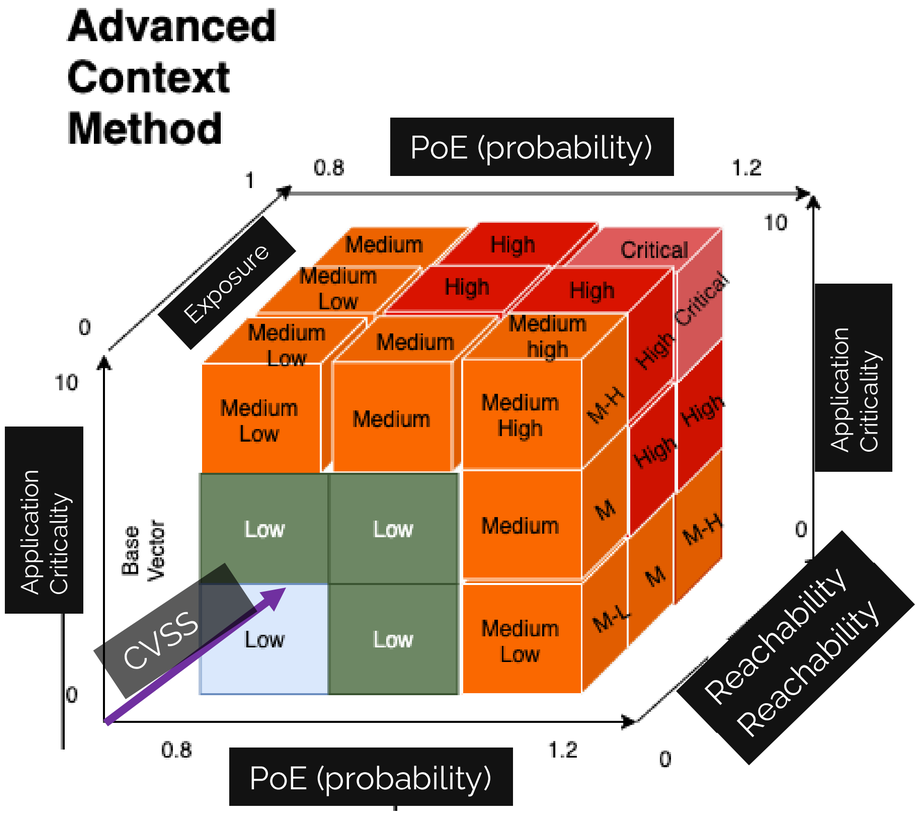
Advanced Context Method



Vulnerability method from past

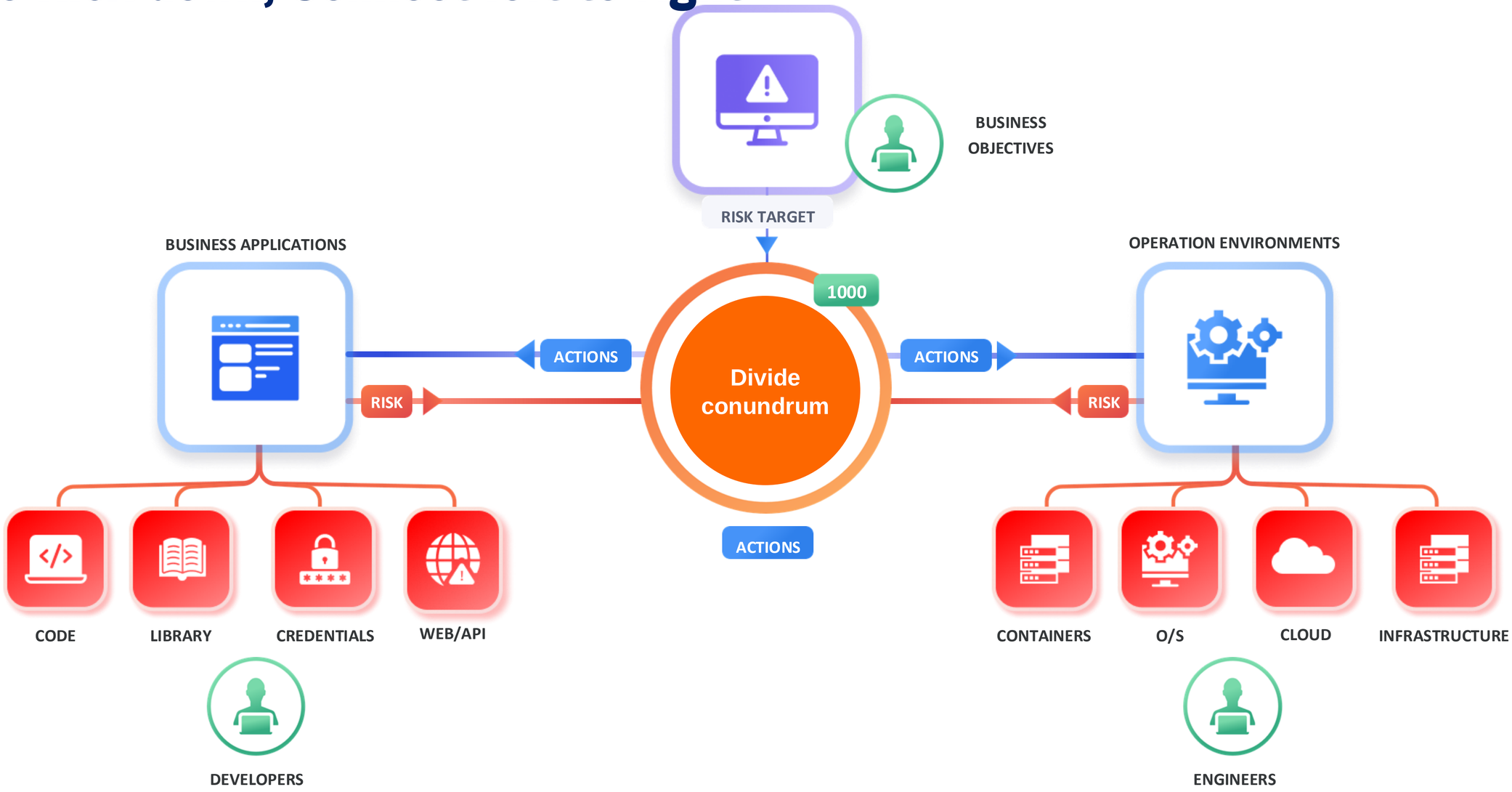
Phoenix 4D Contextual Reachability Risk

PHOENIX BRINGS OUT THE 4TH DIMENSION OF REACHABILITY



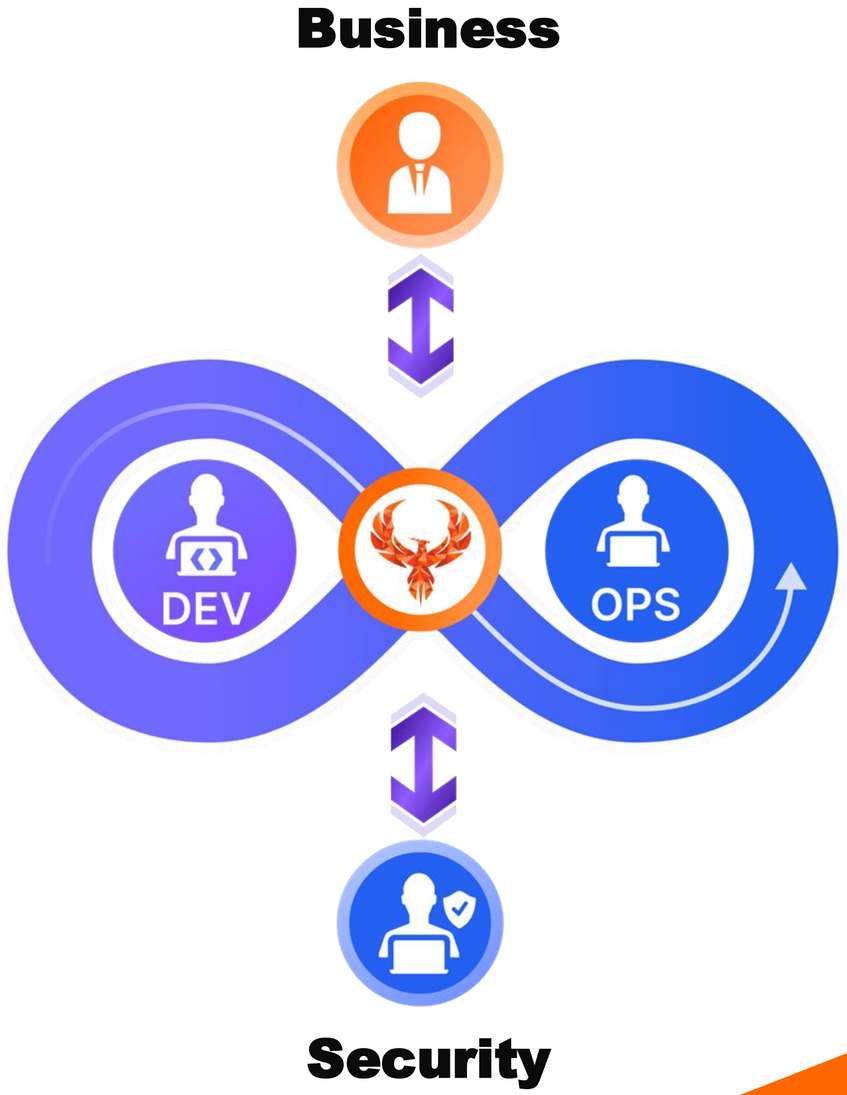
From Number of Vulnerabilities to risk objectives

Drive Risk down, Connect left to right



HOW TO SCALE

SET TARGET THAT ARE ACHIAVABLE INSTEAD OF SLA NEVER REACHED



RISK COMMON LANGUAGE

Code Runtime Attack Path

Reachability analysis

FIX AVAILABLE

THREAT INTEL

EXPLOITABILITY

HOW MANY USERS

HOW IMPORTANT

SEVERITY

PROBABILITY

IMPACT

CONTEXT

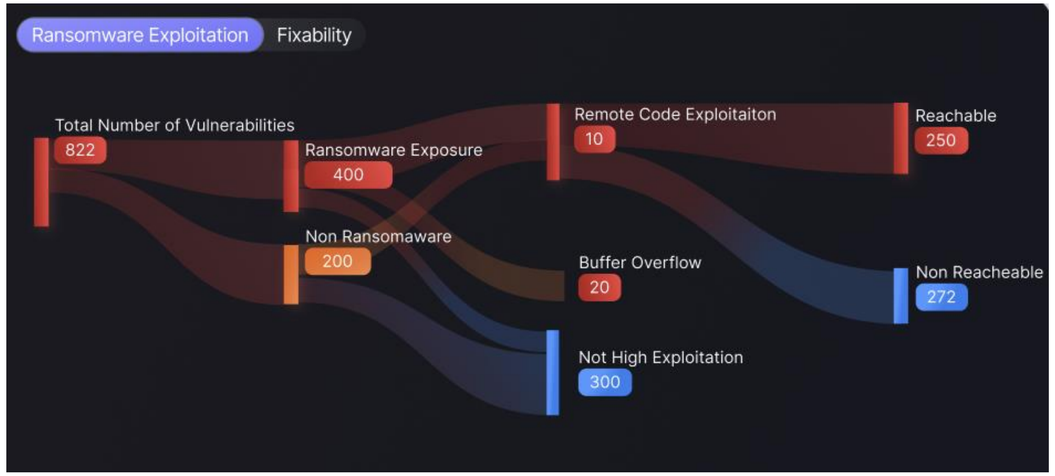
MORE ACCURATE SCORING

Part 3 – A root Cause analysis of vuln

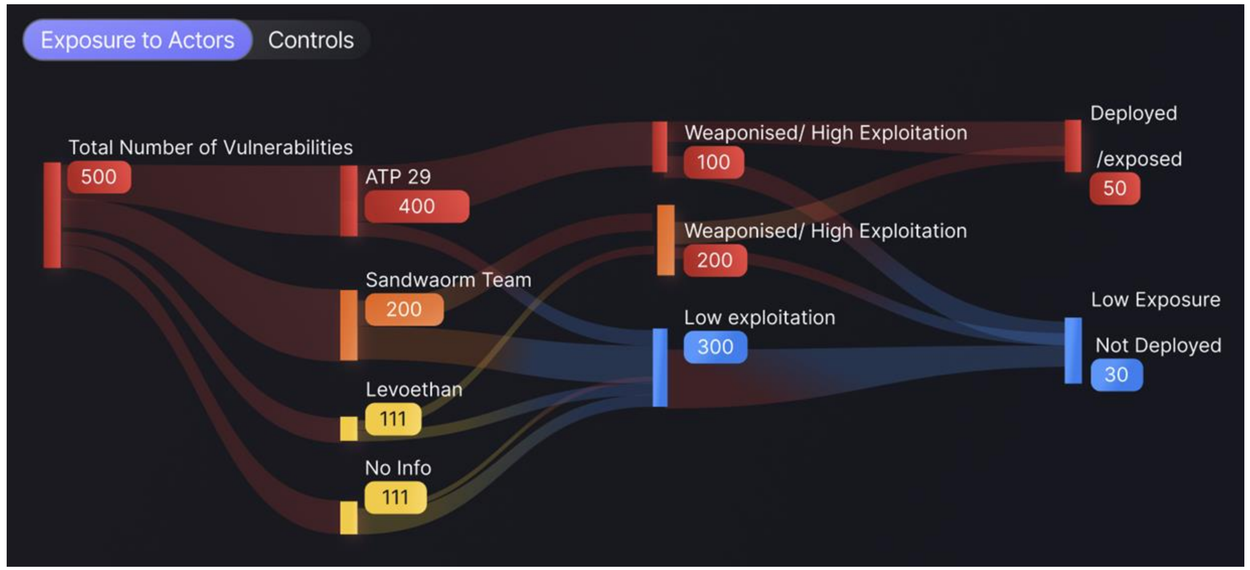
Answering Question – What threat AM I EXPOSED

2025 CVE/FIRST VulnCon

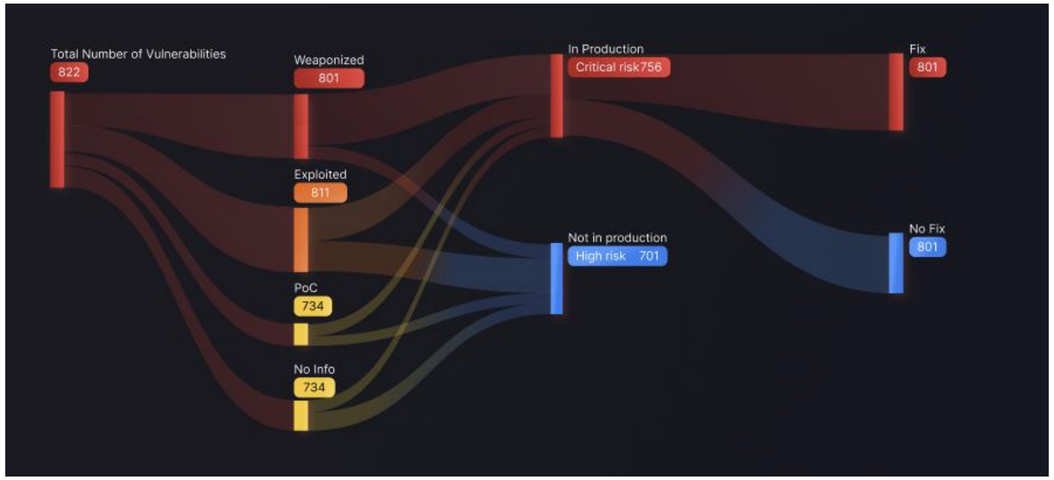
What are your exposure to Ransomware



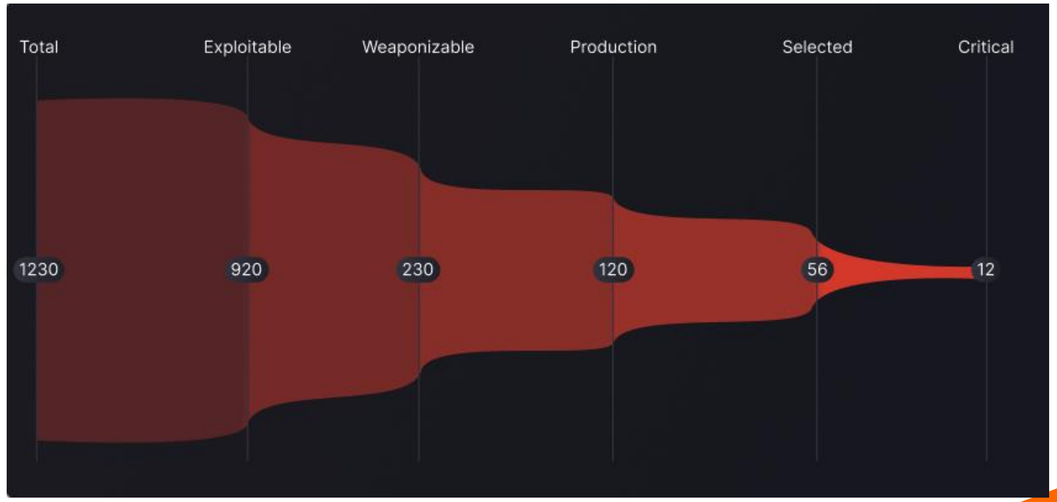
How exposed are you to threat actor X/Y/Z



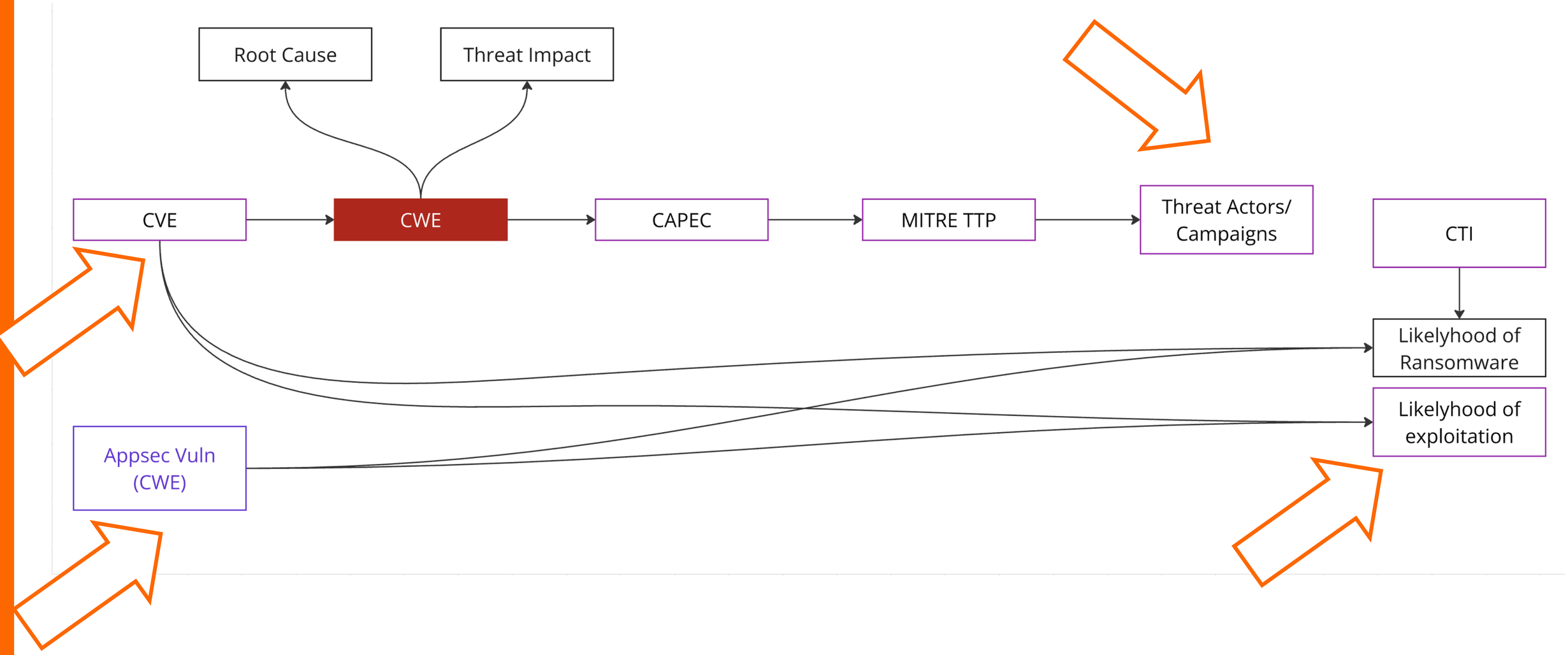
How many exploitable/Weaponizable vulnerability you have



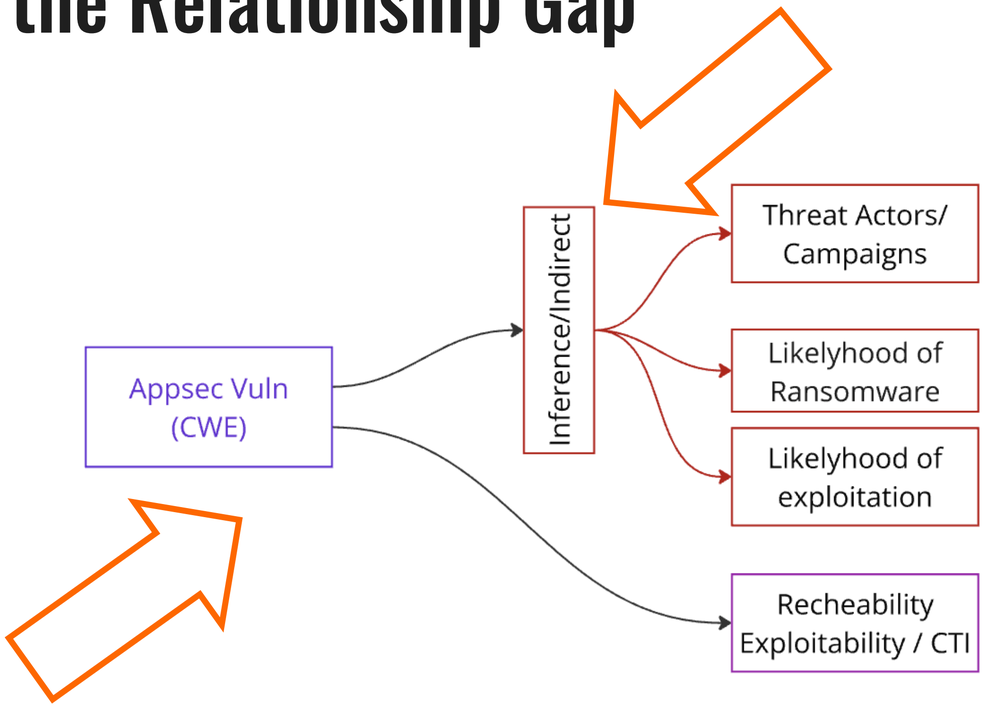
How many Vulnerabilities are actually important



Relationship Gap

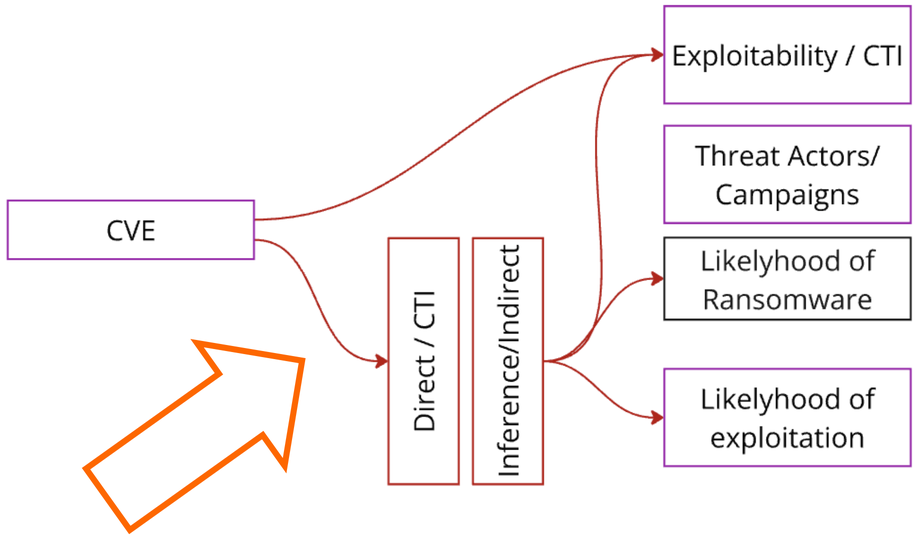


Filling the Relationship Gap



For CWE ? Appsec Vulnerabilities

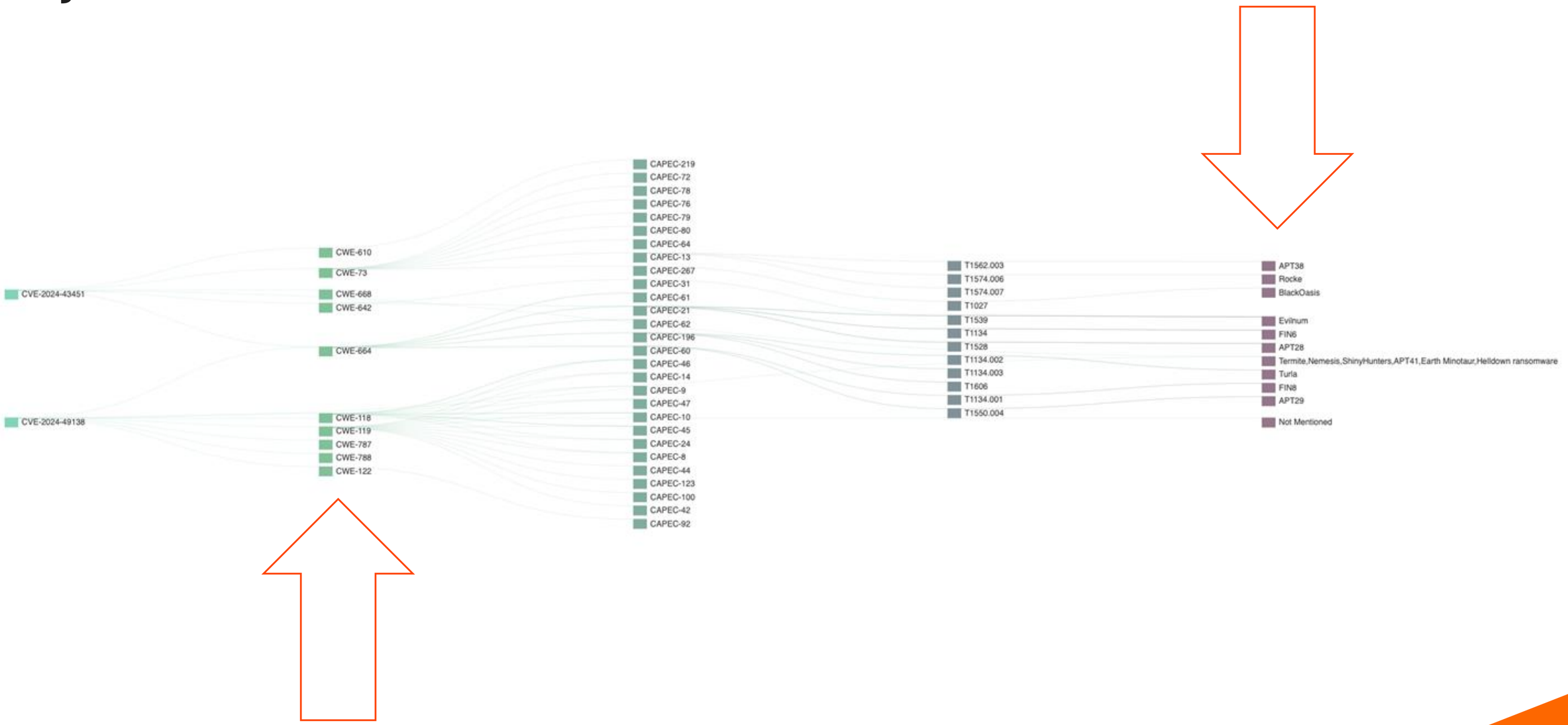
- Knowing the threat actors
- Apply CTI / indirectly
- Knowing possibly of ransomware and exploitation



For CVE based

- Knowing and increasing the coverage CVE – Threat Actor / Technique
- Knowing Which technique is more used
- Use this as probabilistic methods

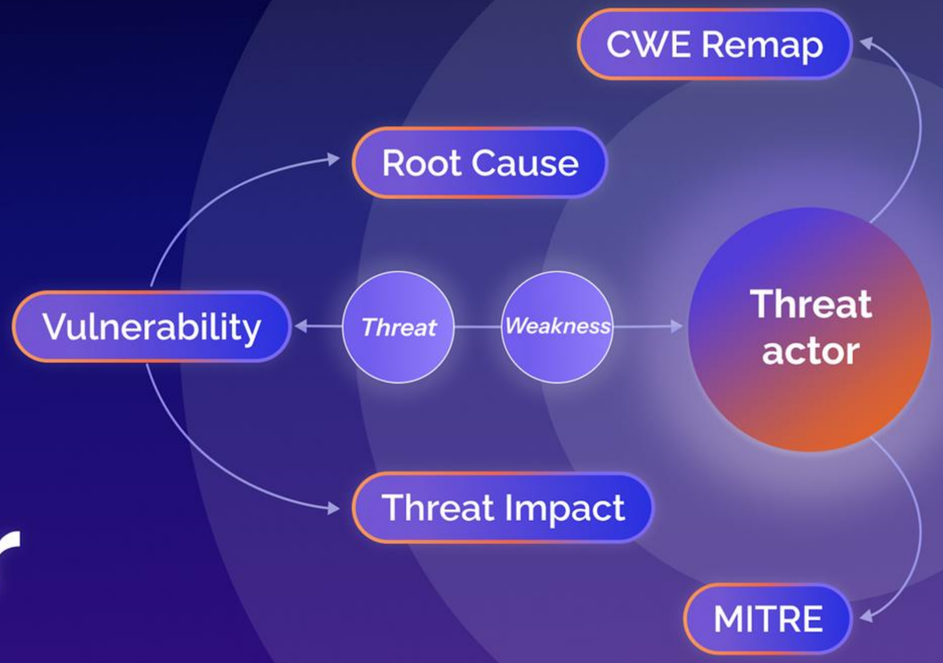
Challenge – Description of vulnerabilities IS NOT root cause analysis

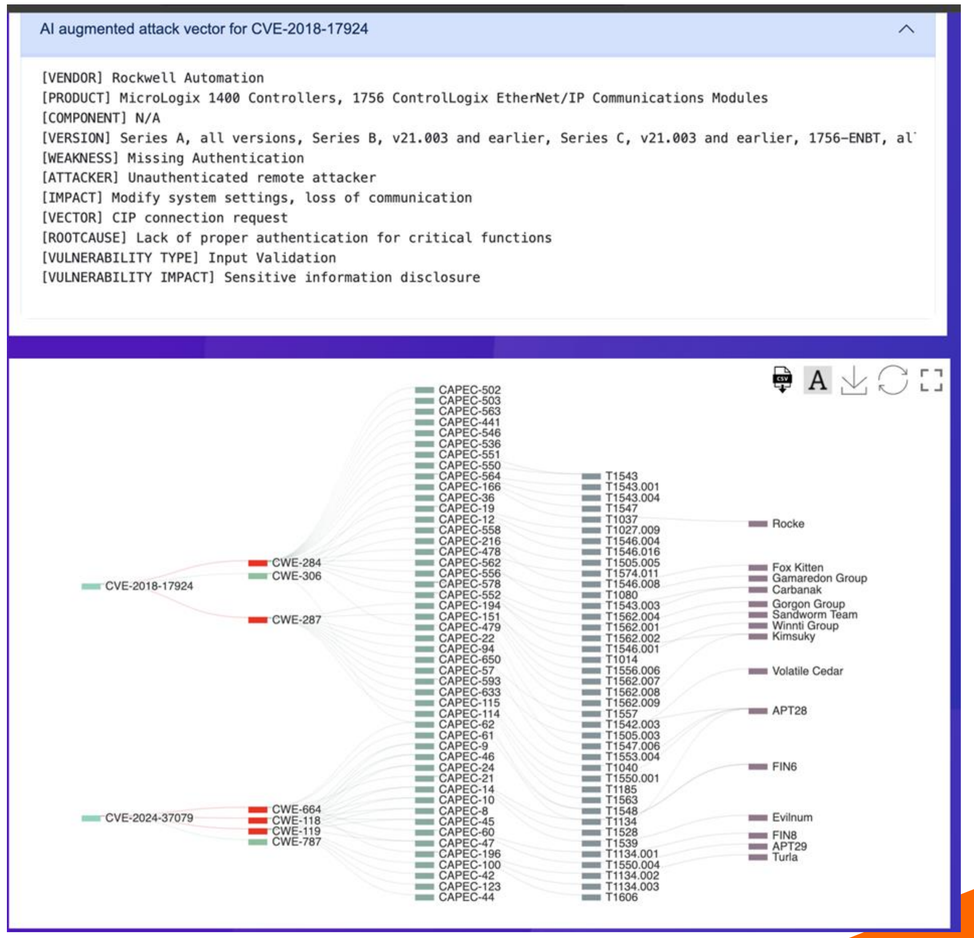


Threat Centric Approach on vulnerabilities

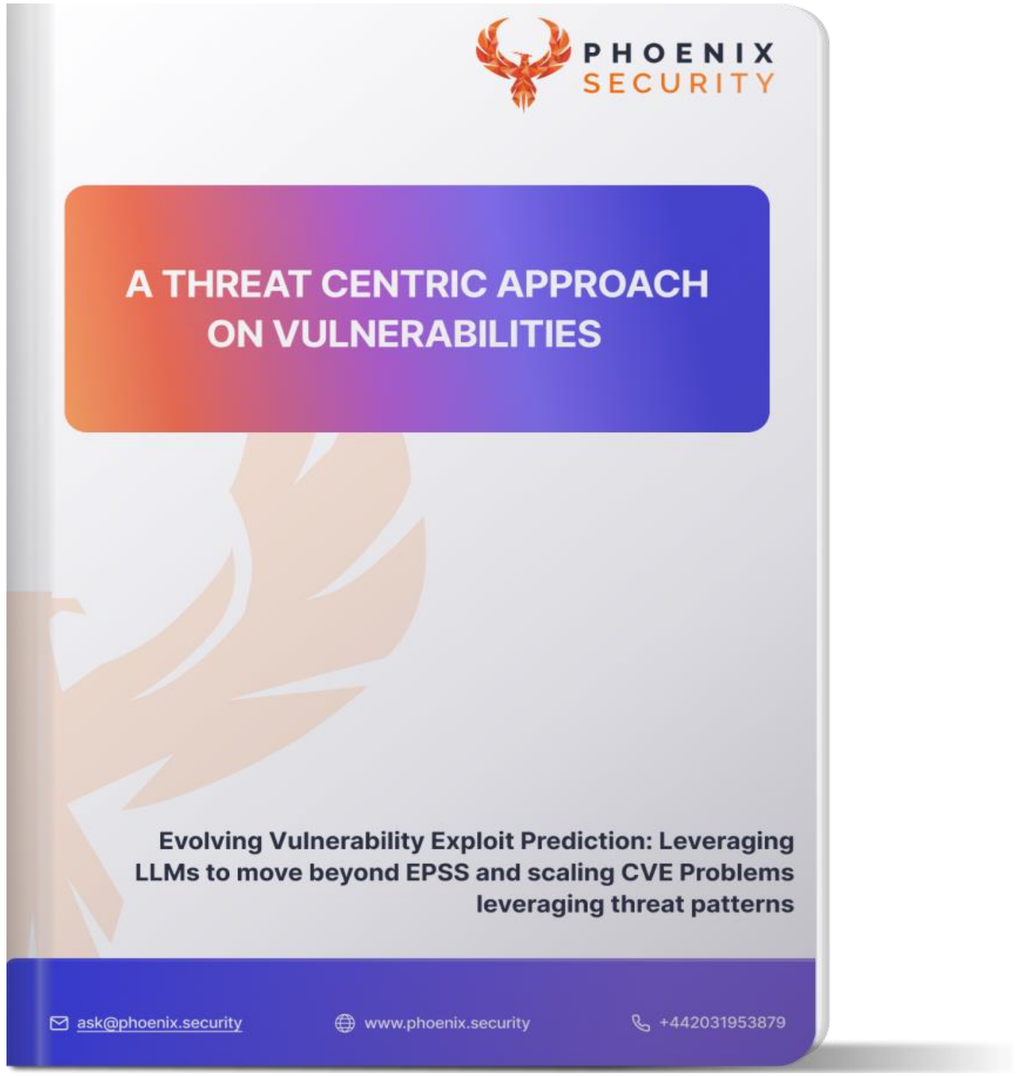
PHOENIX SECURITY

AI Threat centric mapper

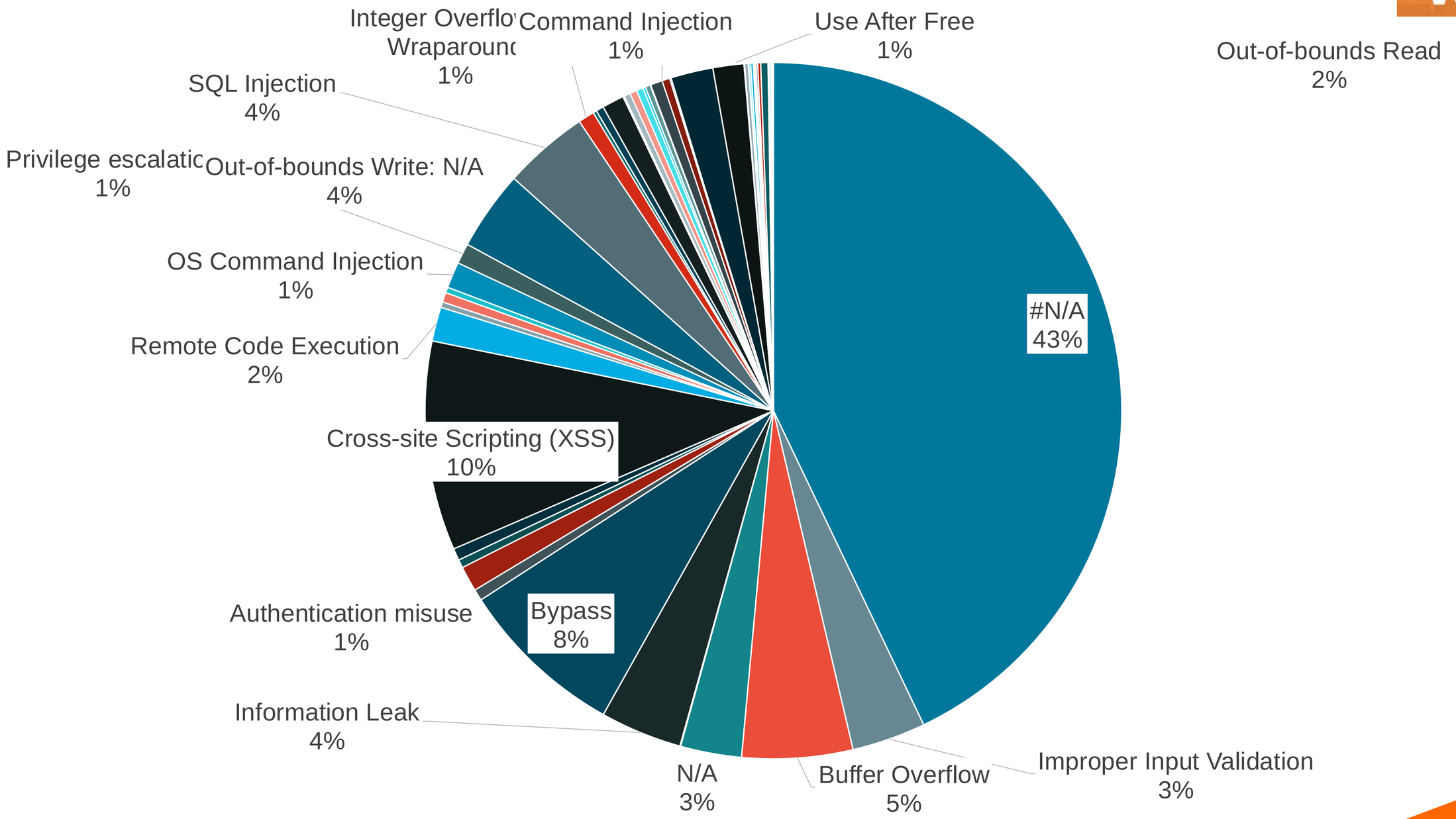




New Whitepaper LLM for a Threat Centric Approach

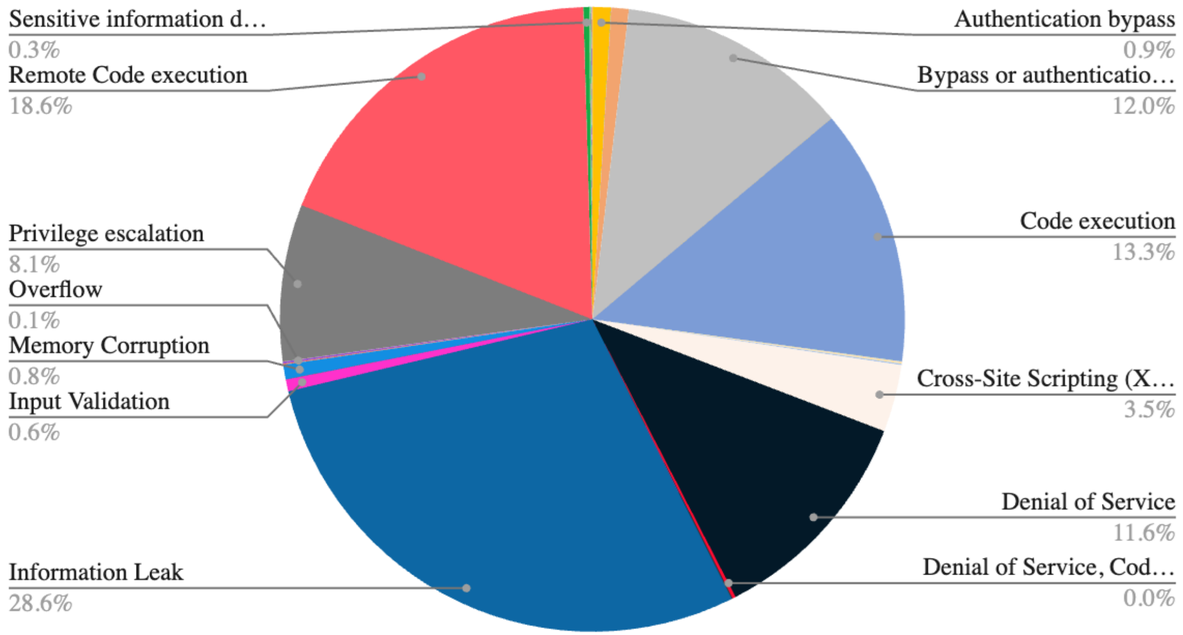


Current CWE Completion – 50% incomplete

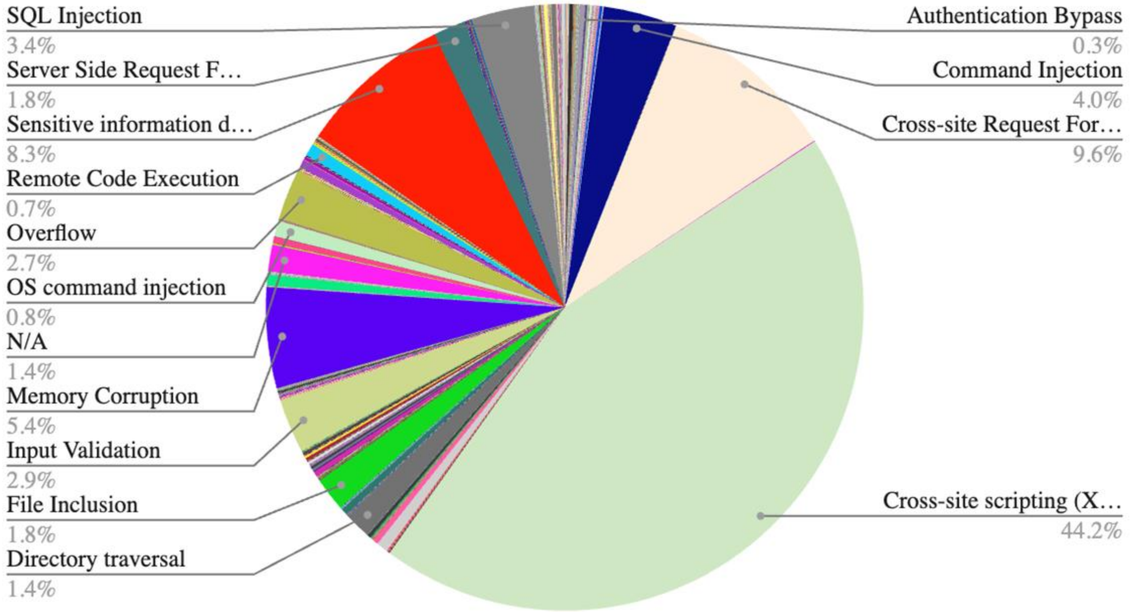


Way Ahead LLM Generation of Simplified Description of vulnerabilities, root cause and technical impact

Threat Root Cause

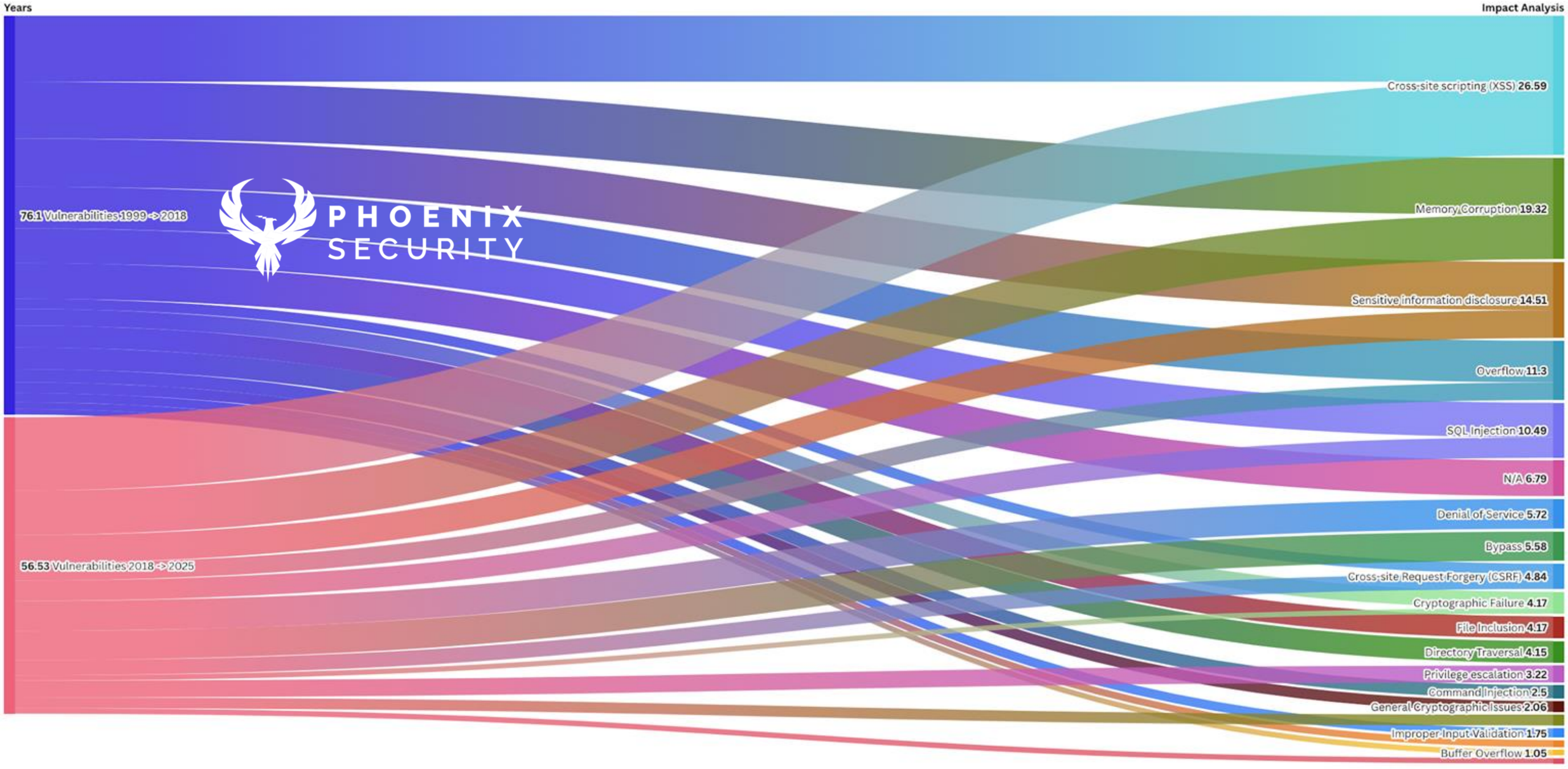


Threat Impact / Weakness



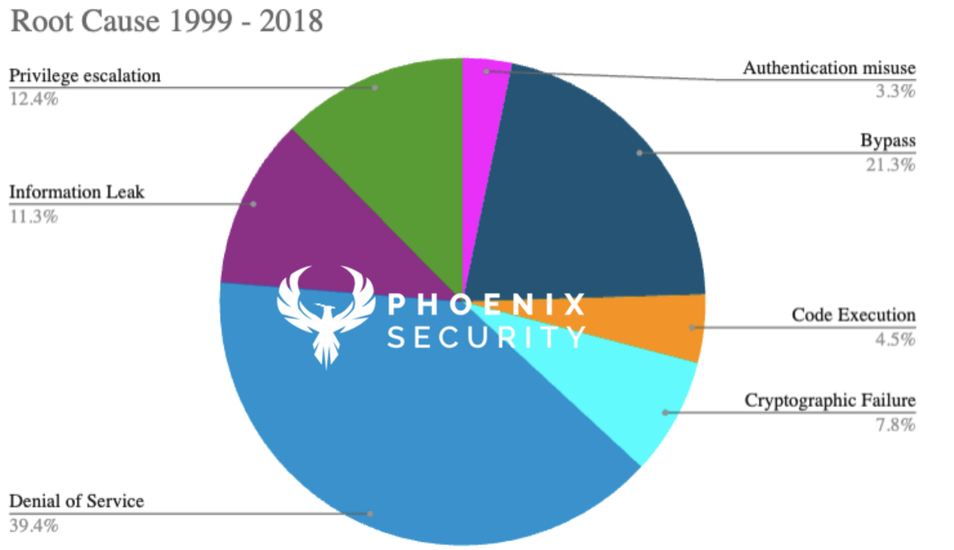
How the Path has changed ... and not -> root cause and...

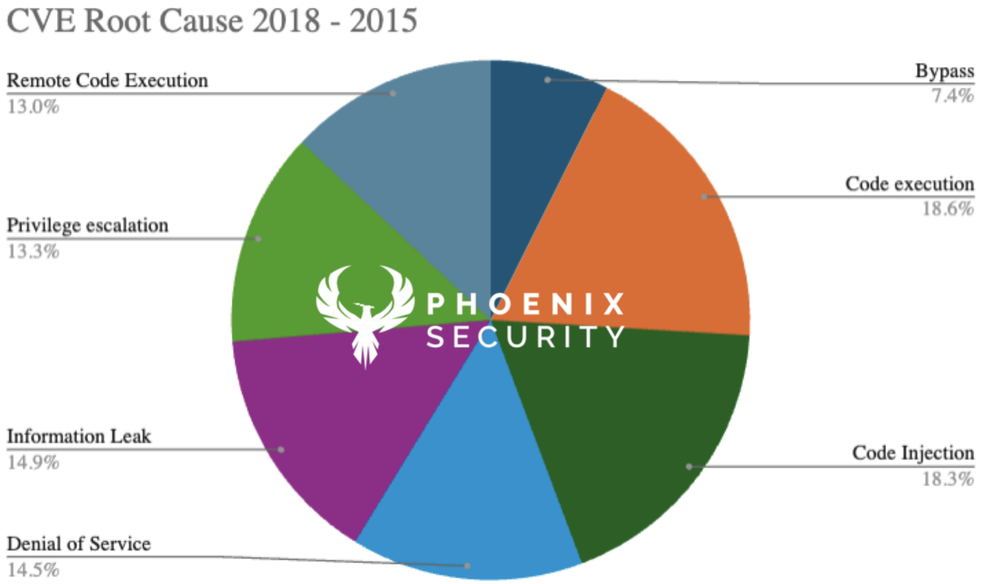
How the Path has changed ... and not -> ...and technical impact



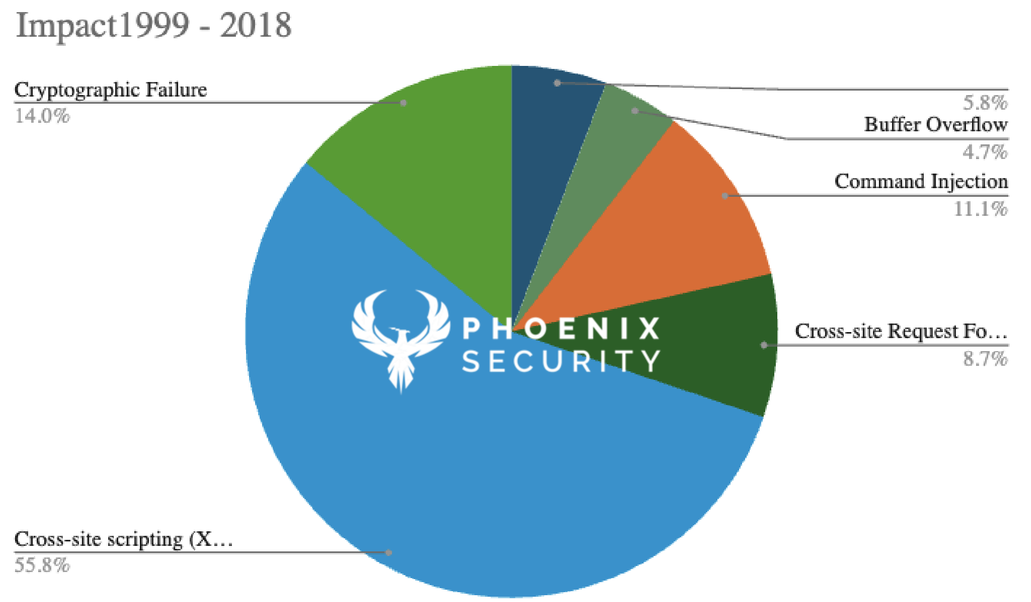
How the threat have evolved

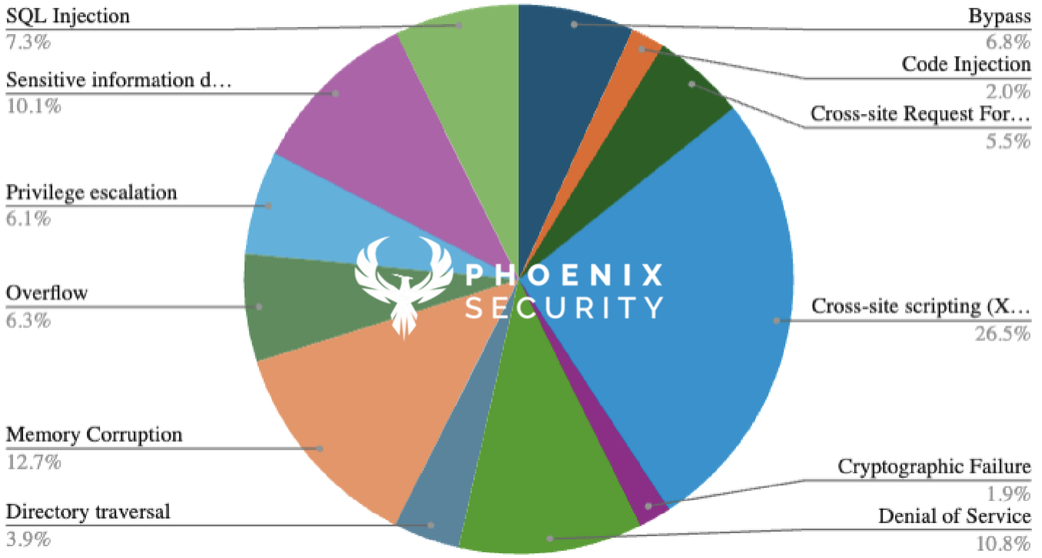
Technical Impact





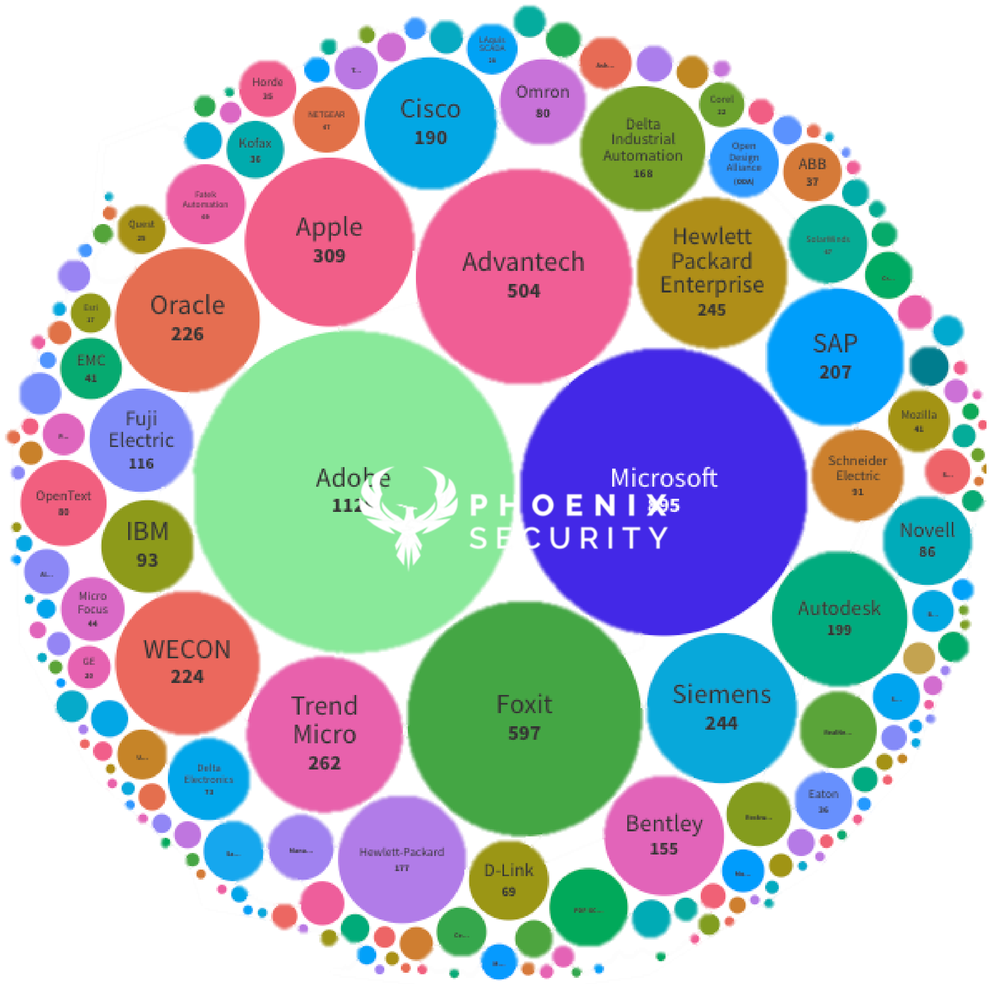
Root Cause / Weakness



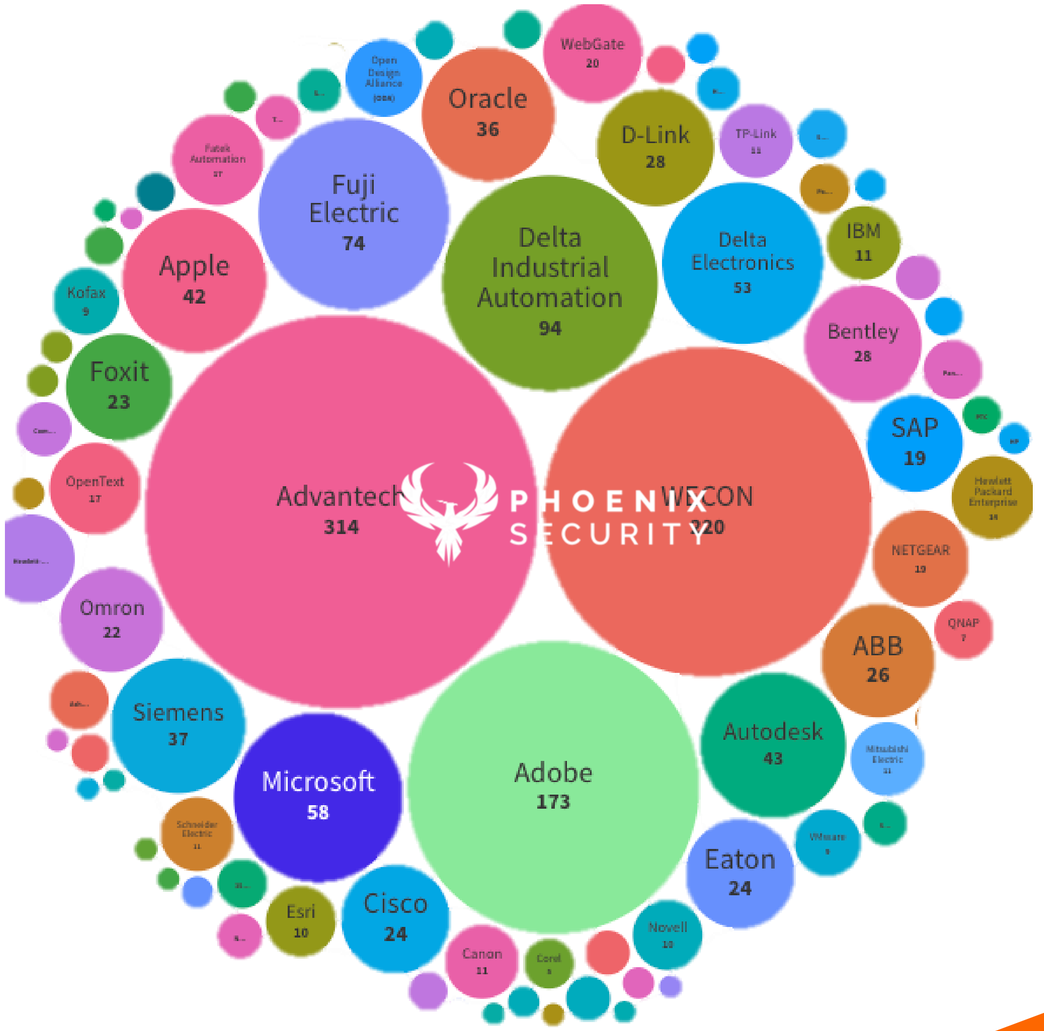


Methodologies of attacks in Zero Days

Root Cause : RCE

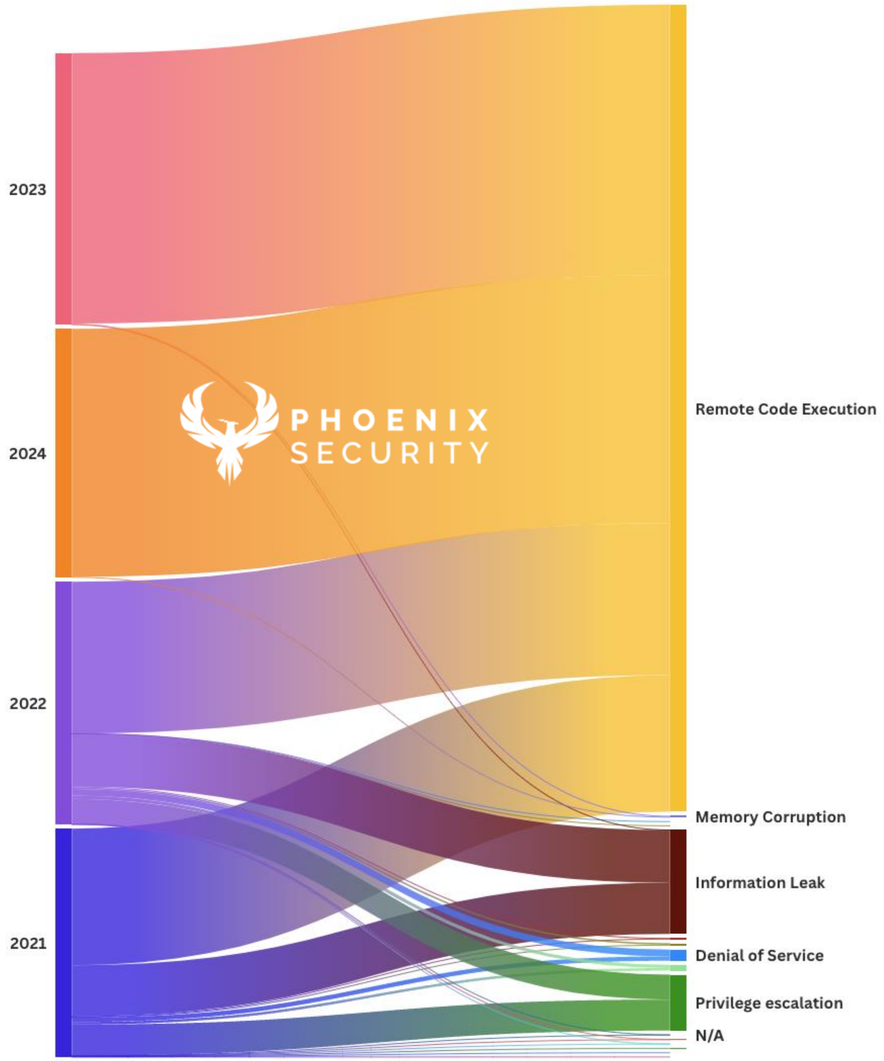


Root Cause : Buffer Overflow

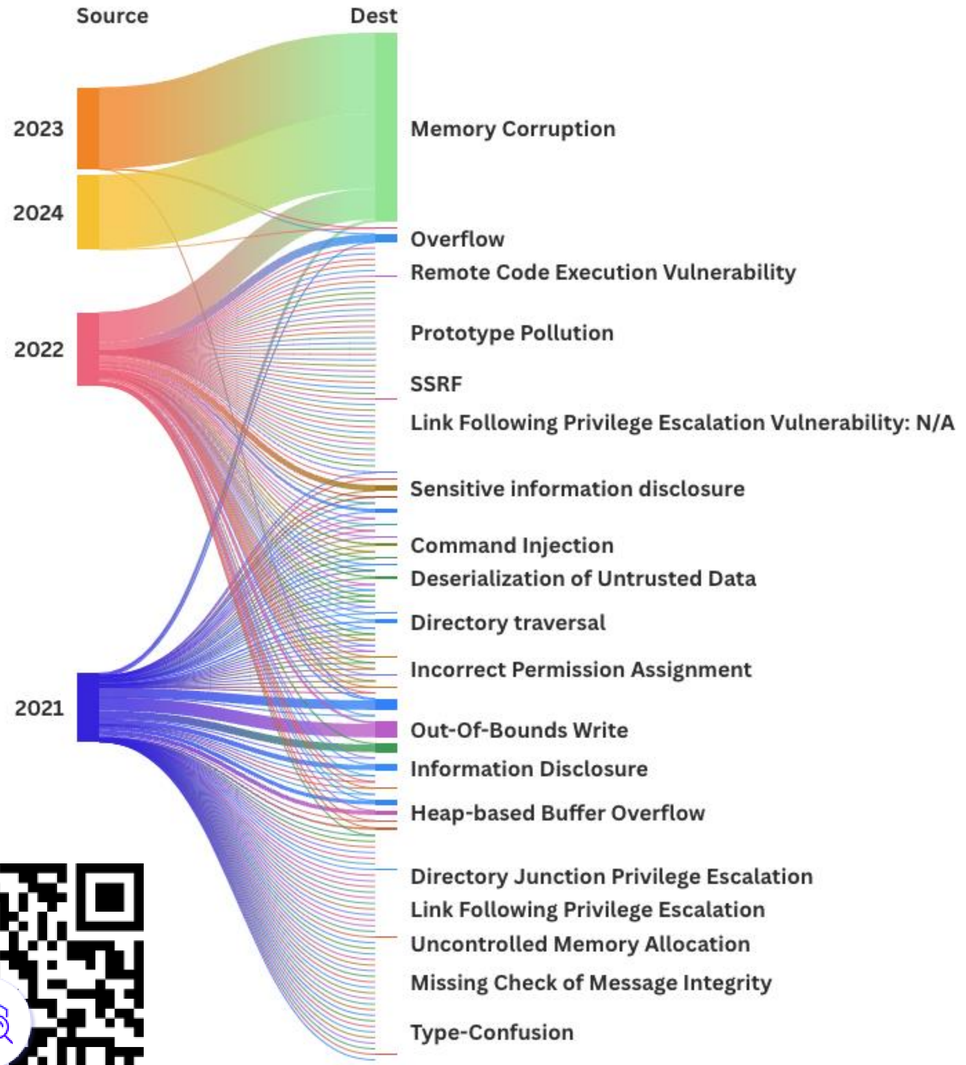


Methodologies of attacks in Zero Days - Weakness

Root Cause : RCE

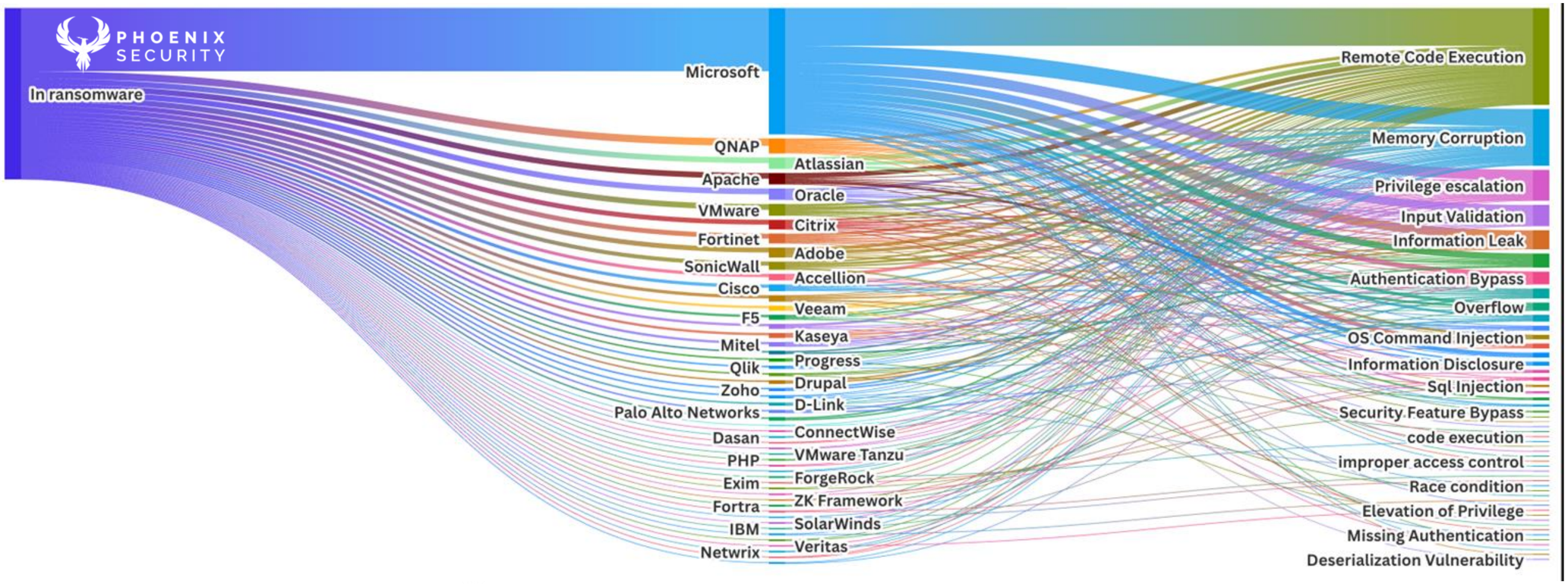


Technical Impact: Mem Corruption



Methodologies of attacks in Ransomware

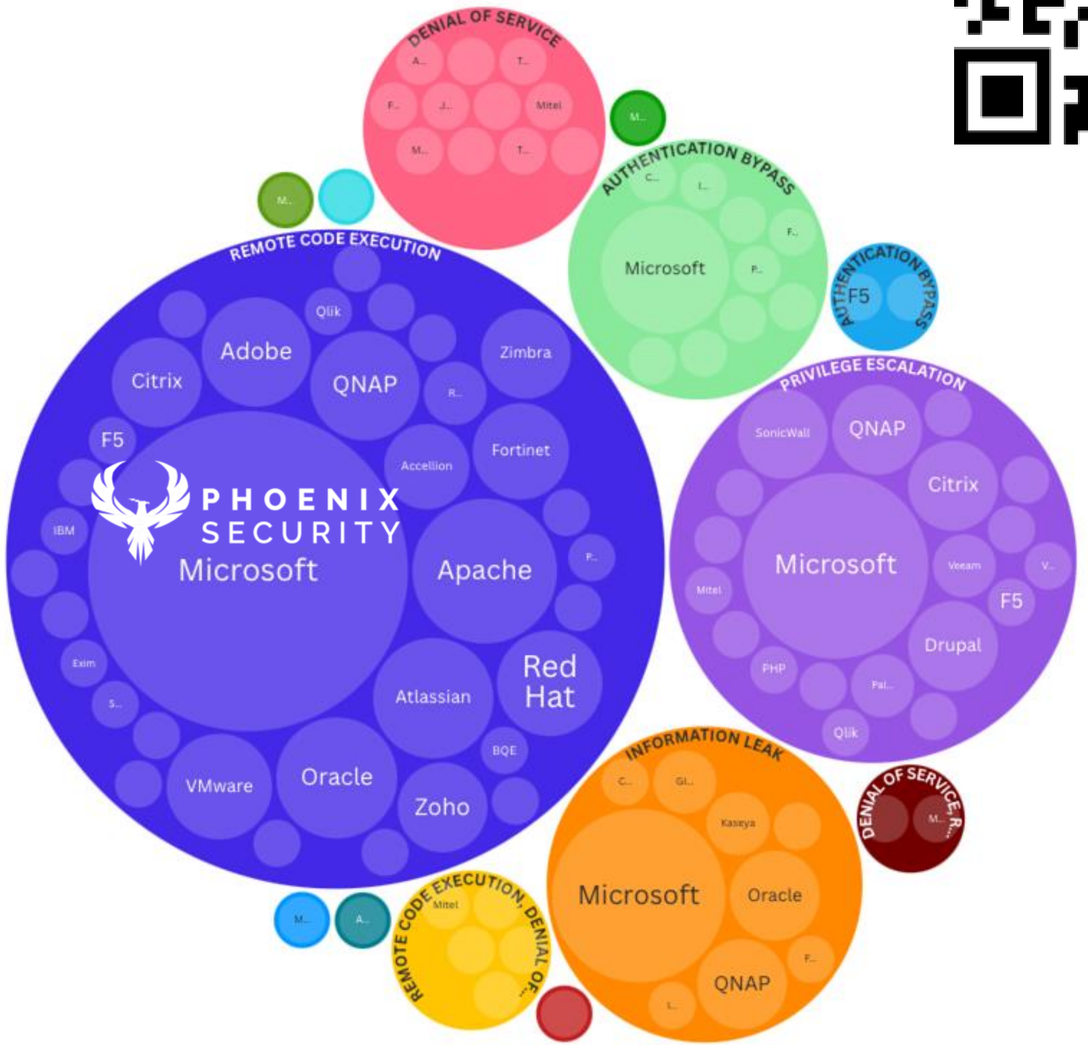
2025 CVE/FIRST VulnCon



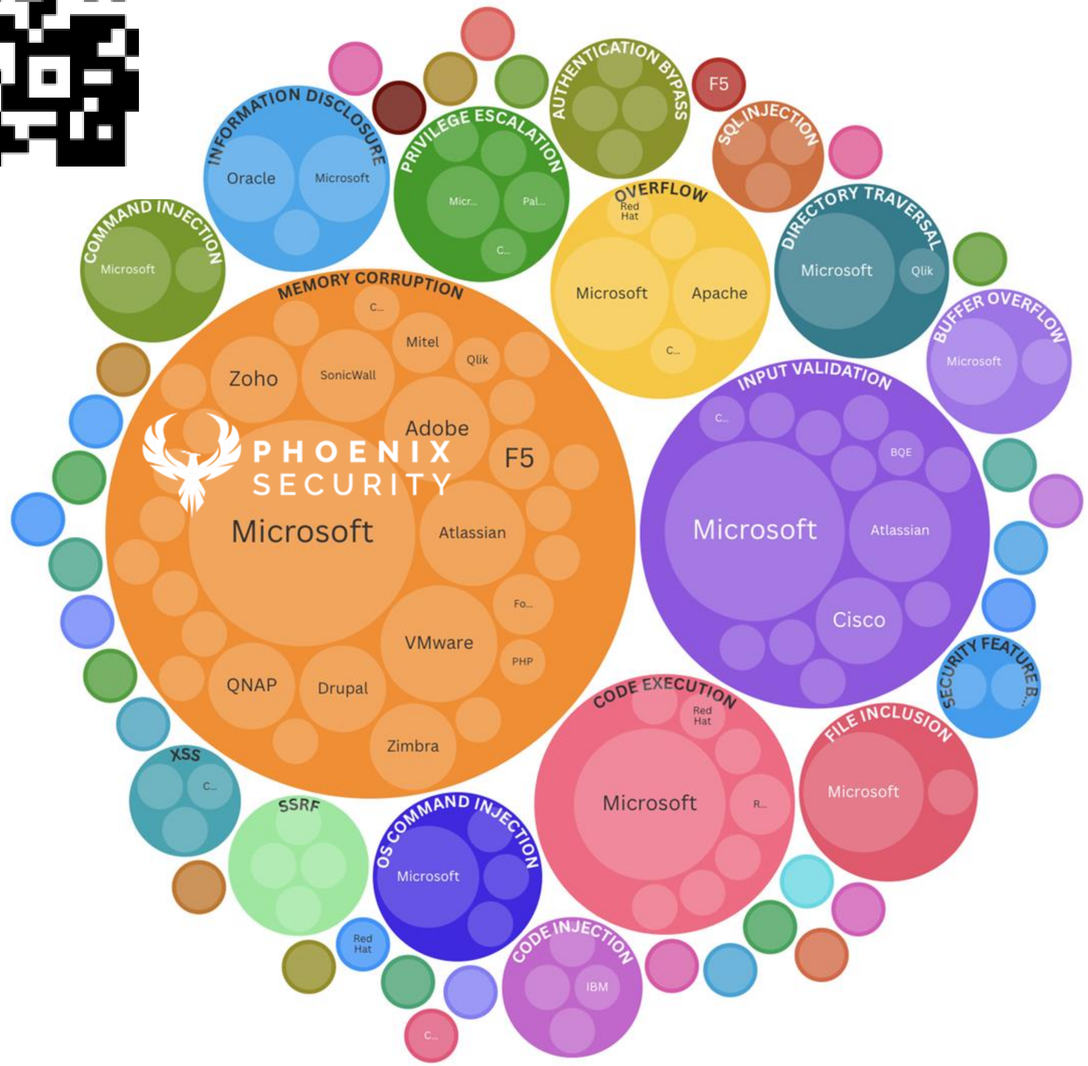
Methodologies of attacks in Ransomware

2025 CVE/FIRST VulnCon

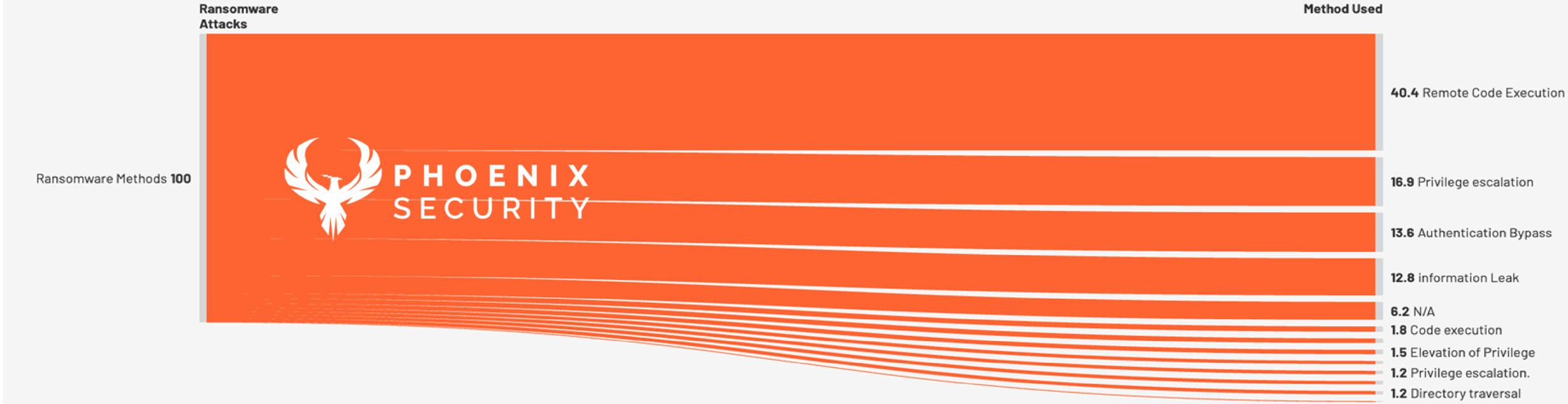
Technical Impact



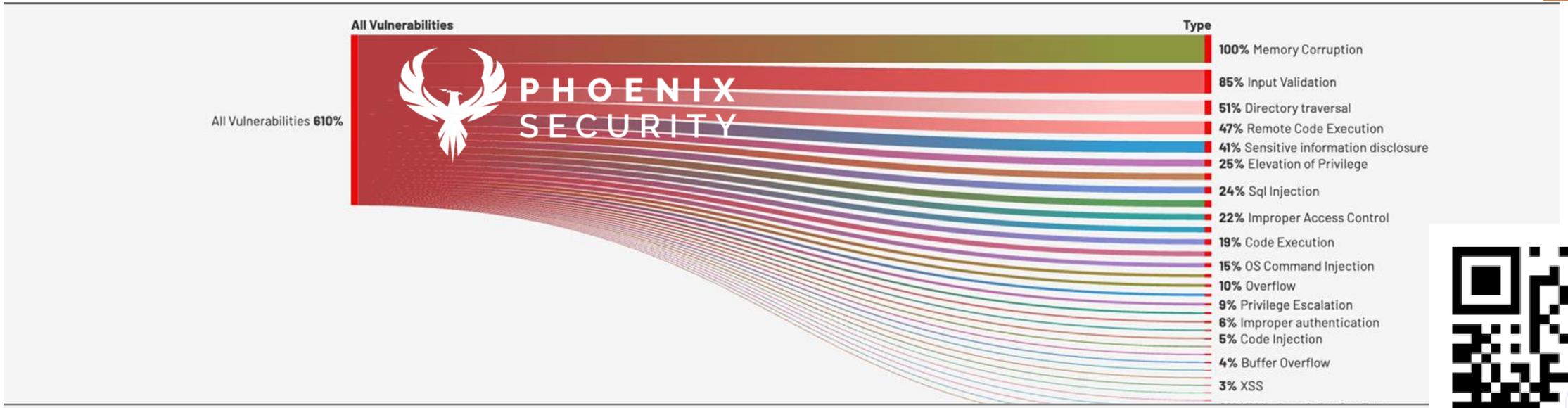
Root Cause

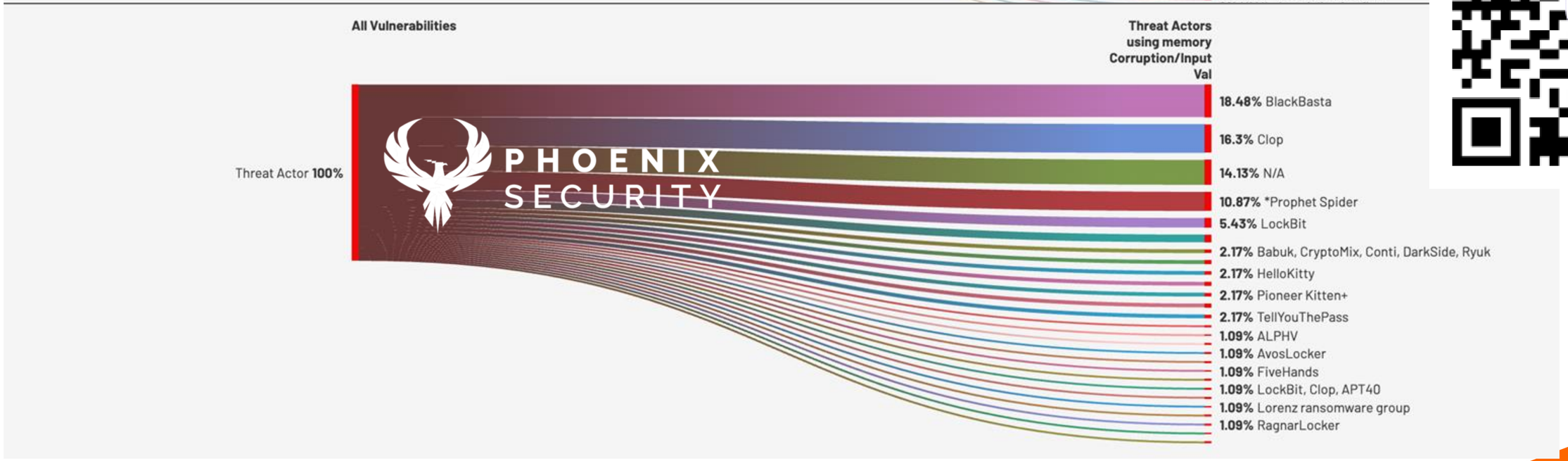


Methodologies of attacks in Ransomware



Impact of attacks in Ransomware

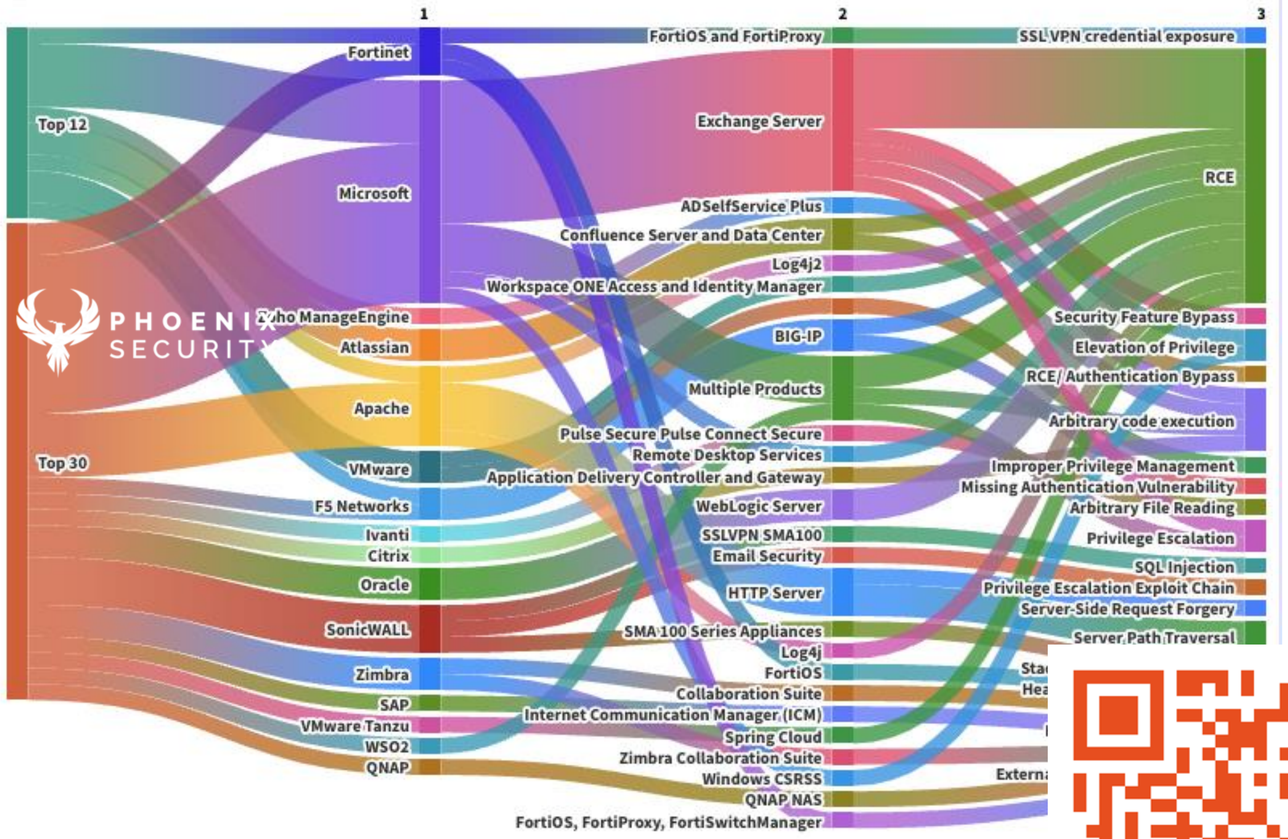




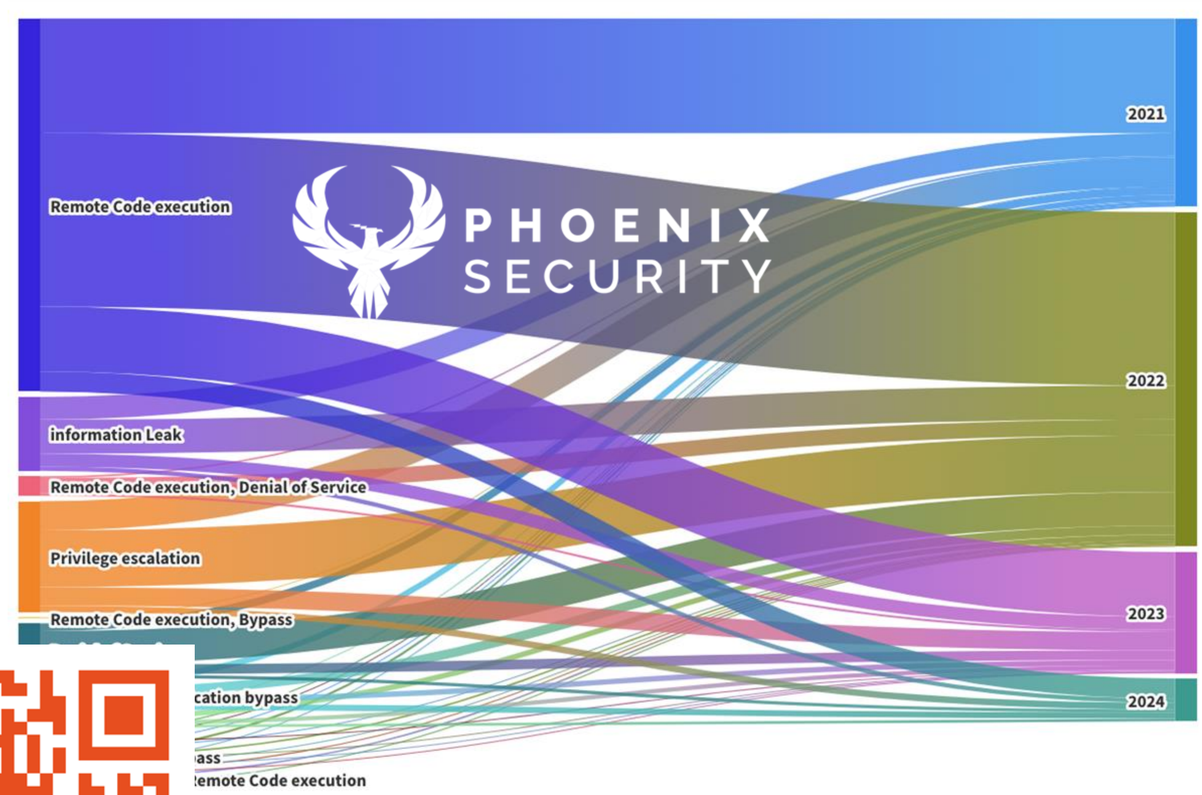
2025 CVE/FIRST VulnCon

Phoenix CTI - MOST USED ATTACK METHODS

TOP EXPLOITS METHODS



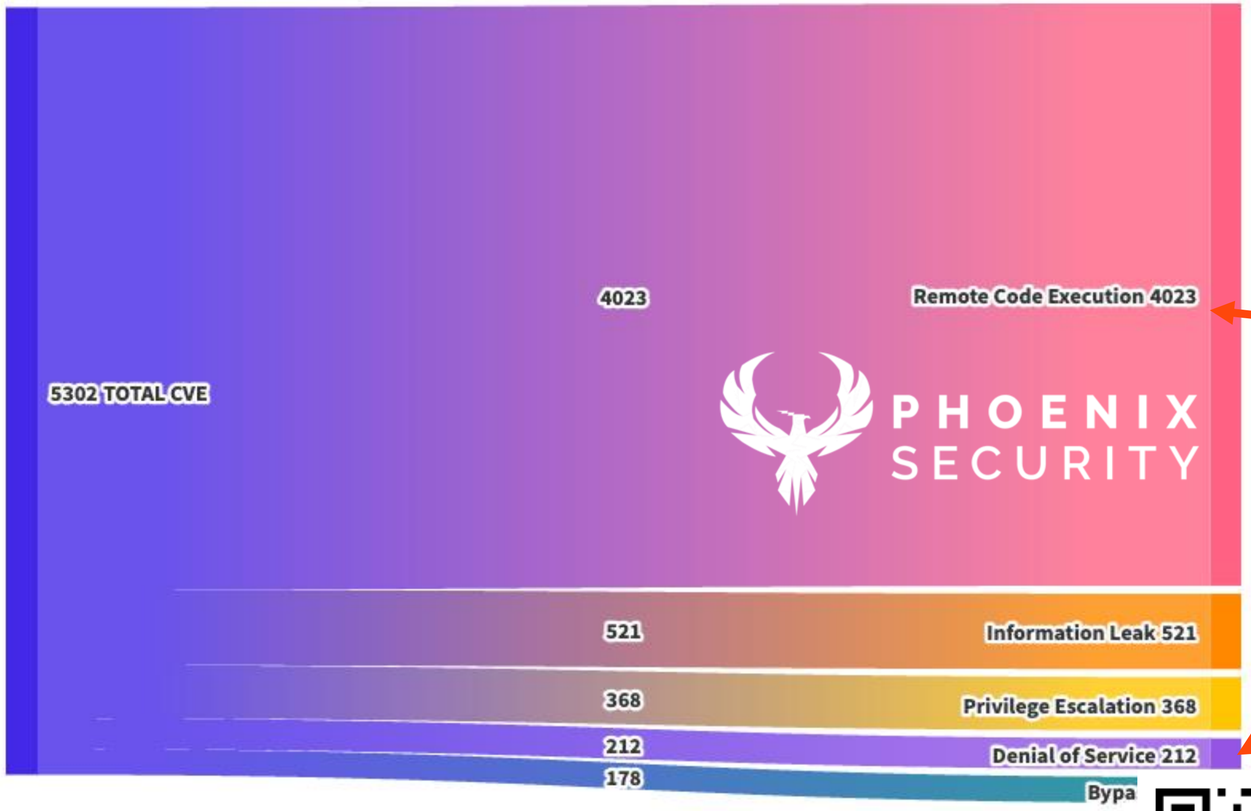
CISA KEV



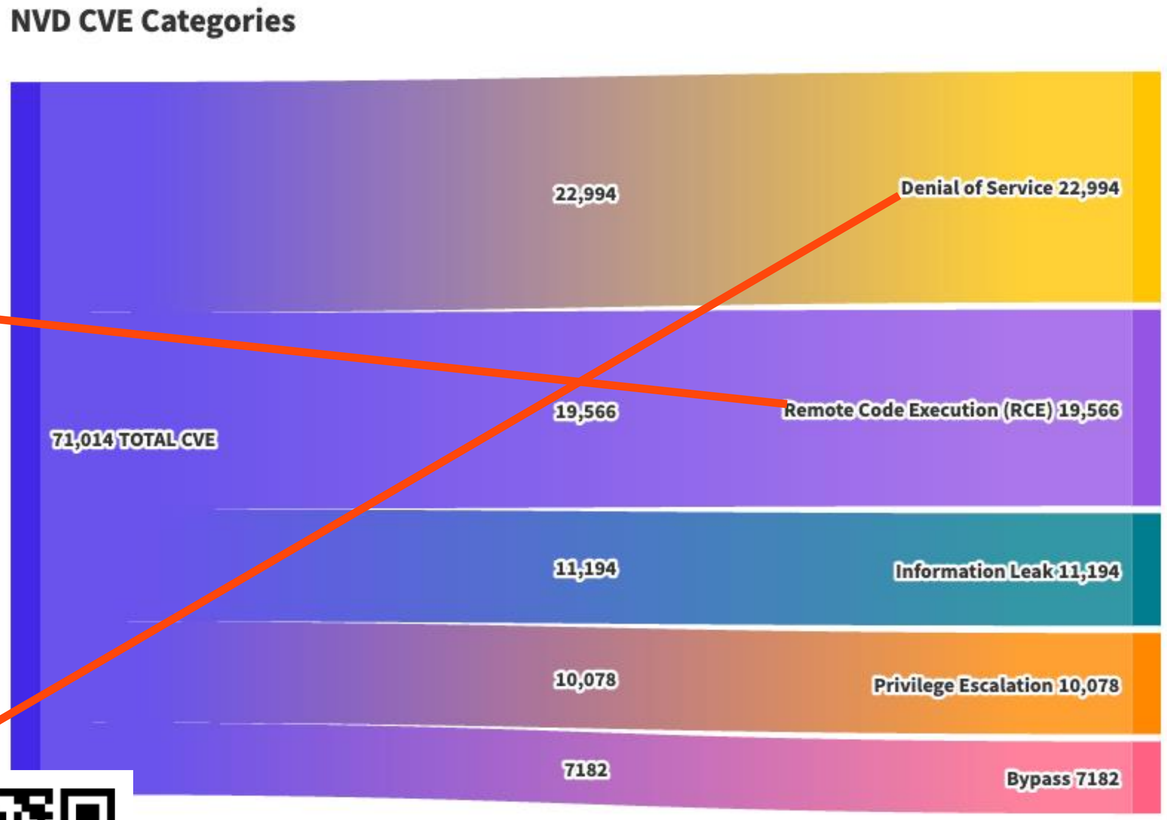
Phoenix CTI – Github PoC – Most used Method

2025 CVE/FIRST VulnCon

TOP EXPLOITS METHODS



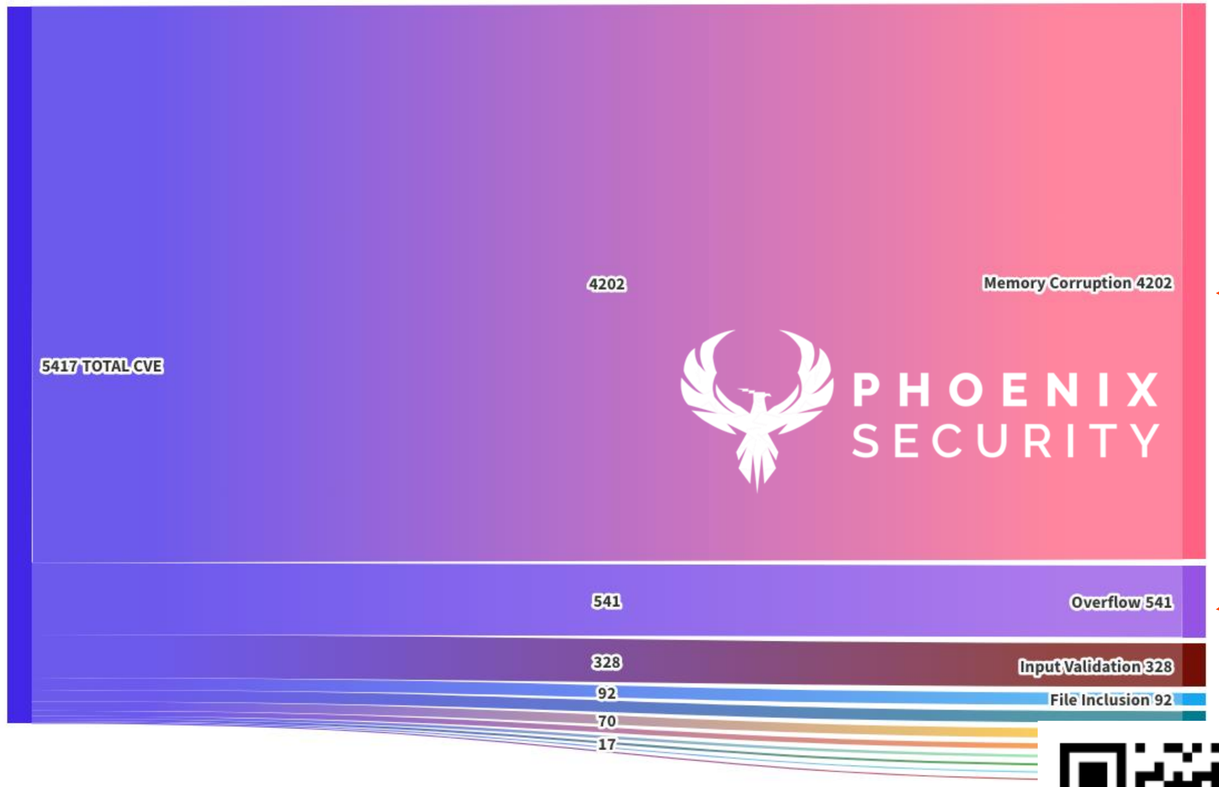
Overall NVD



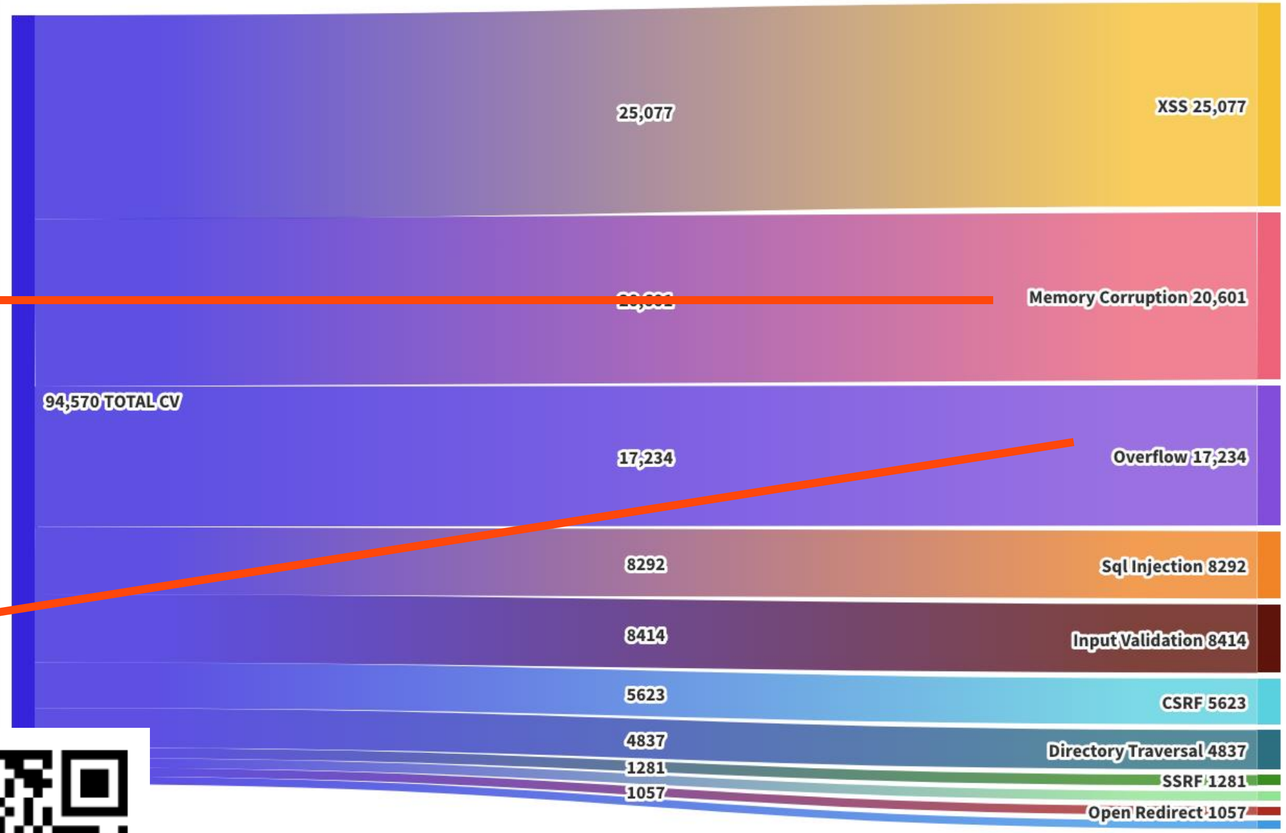
Phoenix CTI – Github PoC – prevalent technical impact

2025 CVE/FIRST VulnCon

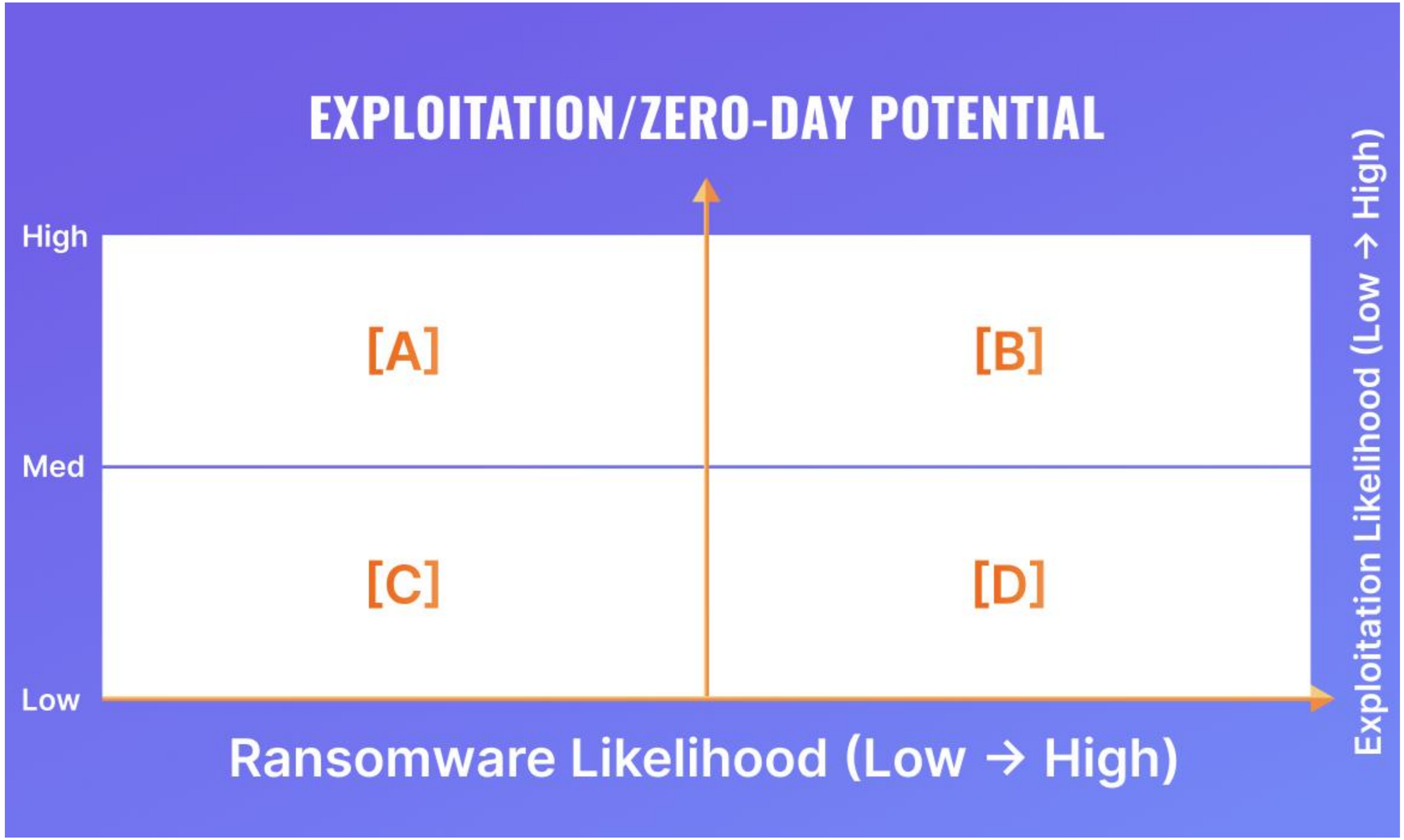
TOP EXPLOITS IMPACT



Overall NVD

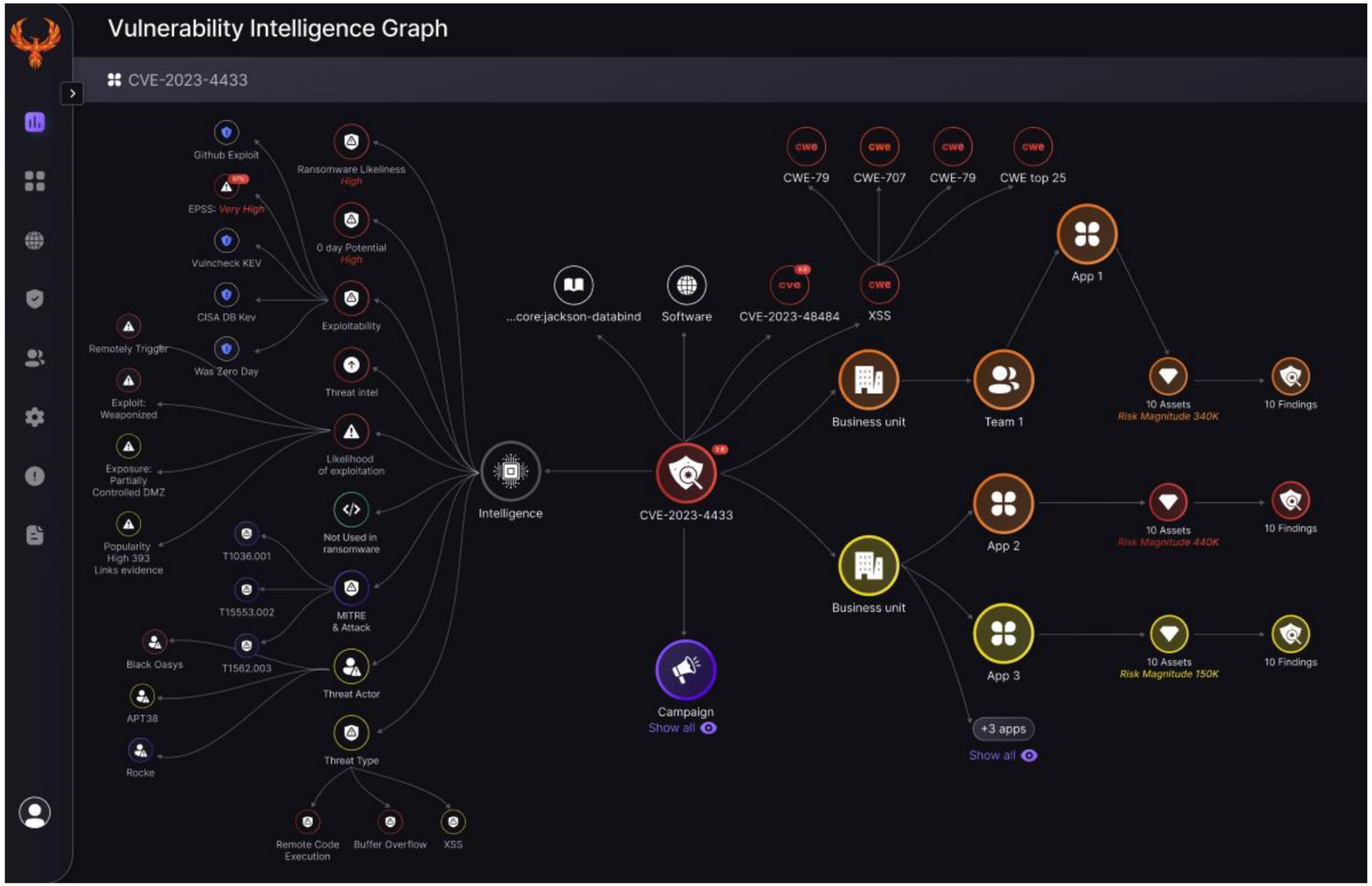


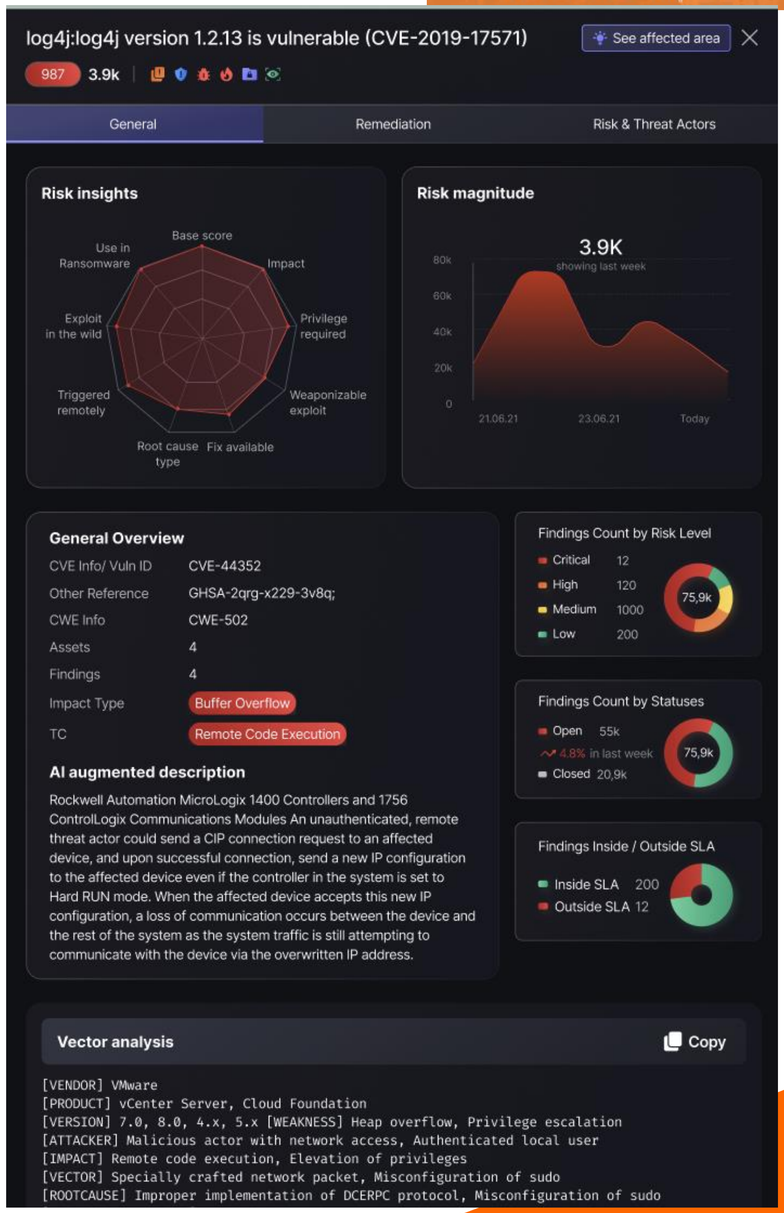
Phoenix – Introducing the world first threat centric approach on vulnerability



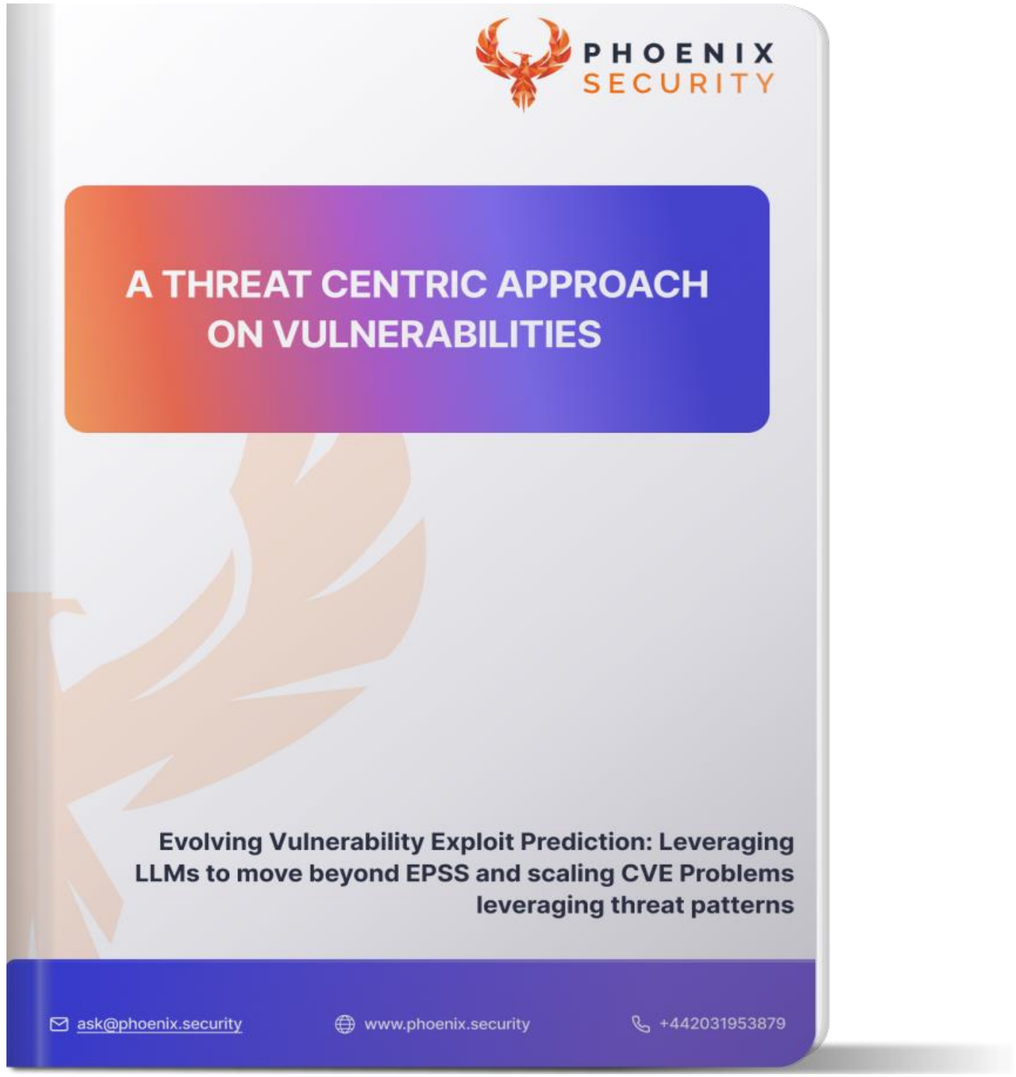
Releasing the new Threat Centric Approach on vulnerabilities

Phoenix - Vulnerability Intelligence, Evolution and new Vector





How we did it - New eBook - Threat Centric Approach



Conclusions

So we solved security right?

There is a light at the end of the tunnel

- There is no silver bullet (duh)
- Application Security + Environment is not new is the only solution
- Security Engineering + Vulnerability Management = THE SILVER BULLET
- From reactive to proactive > ANOTHER SILVER BULLET

PHOENIX
SECURITY

ACT ON CONTAINER VULN

ACT ON ENDPOINT VULN

ACT ON CLOUD VULN

CONTEXTUALIZE, PRIORITIZE & ACT ON RISK

ACT ON APPSEC VULN

ACT ON INFRA VULN

ACT ON CODE VULN

ACT ON SBOM VULN

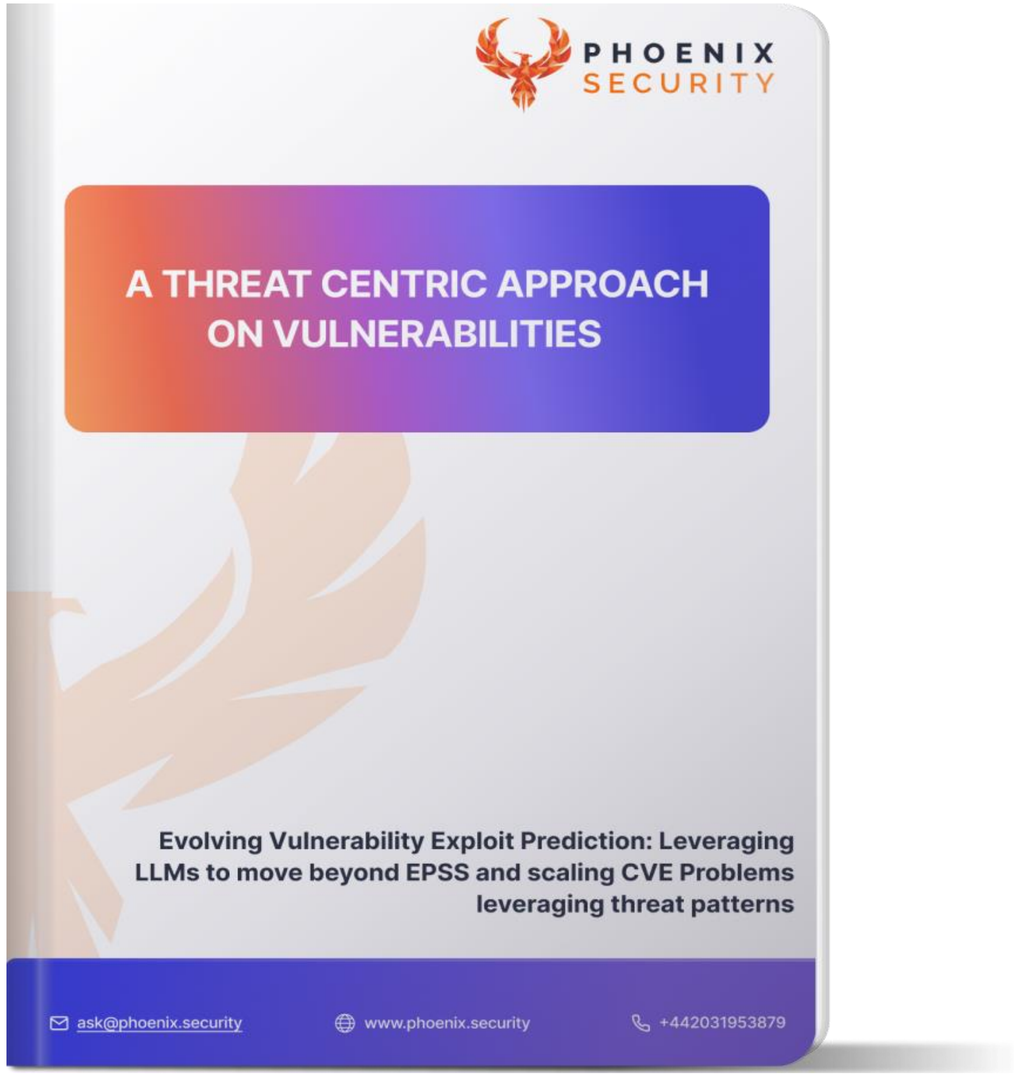
Phoenix Security Unify ASPM & CSPM for a contextual approach

2025 CVE/FIRST VulnCon

IDENTIFY PROBLEMS | **ORGANIZE, PRIORITIZE, CONTEXTUALIZE** | **ACTIONS ON RISK**

Releasing the new Threat Centric Approach on vulnerabilities

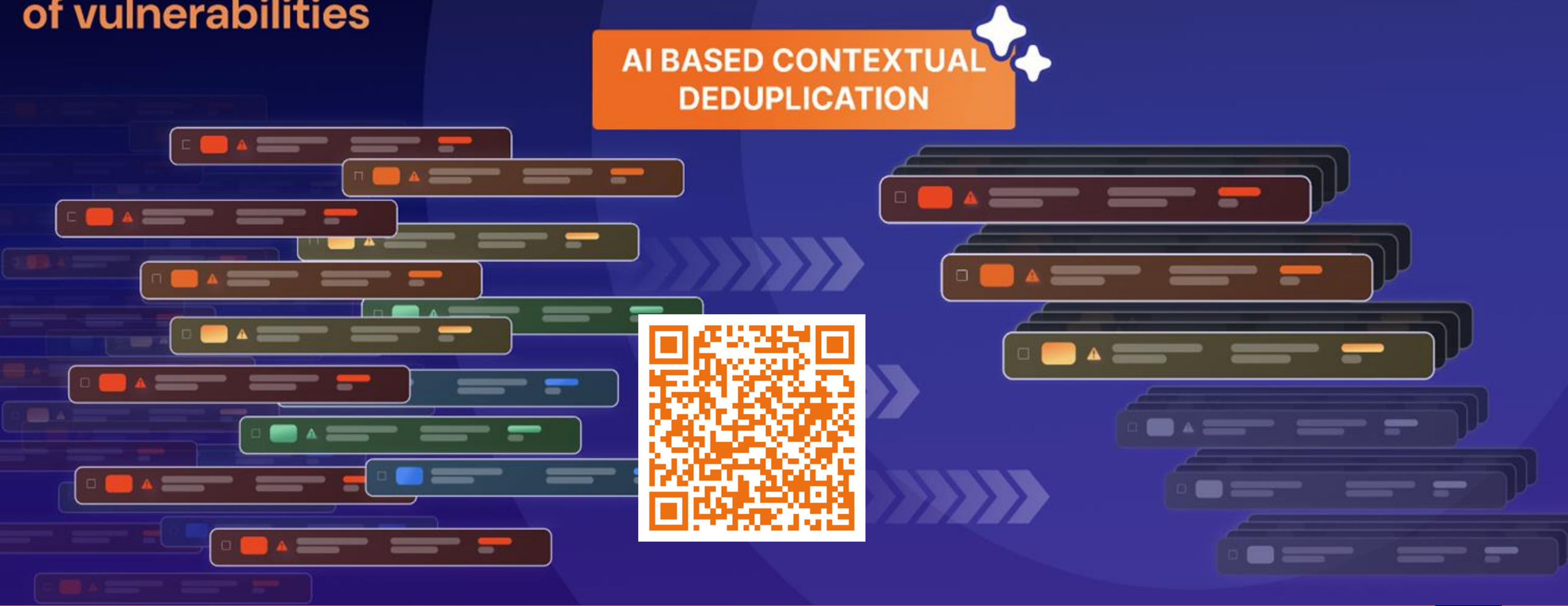
New eBook LLM for a Threat Centric Approach



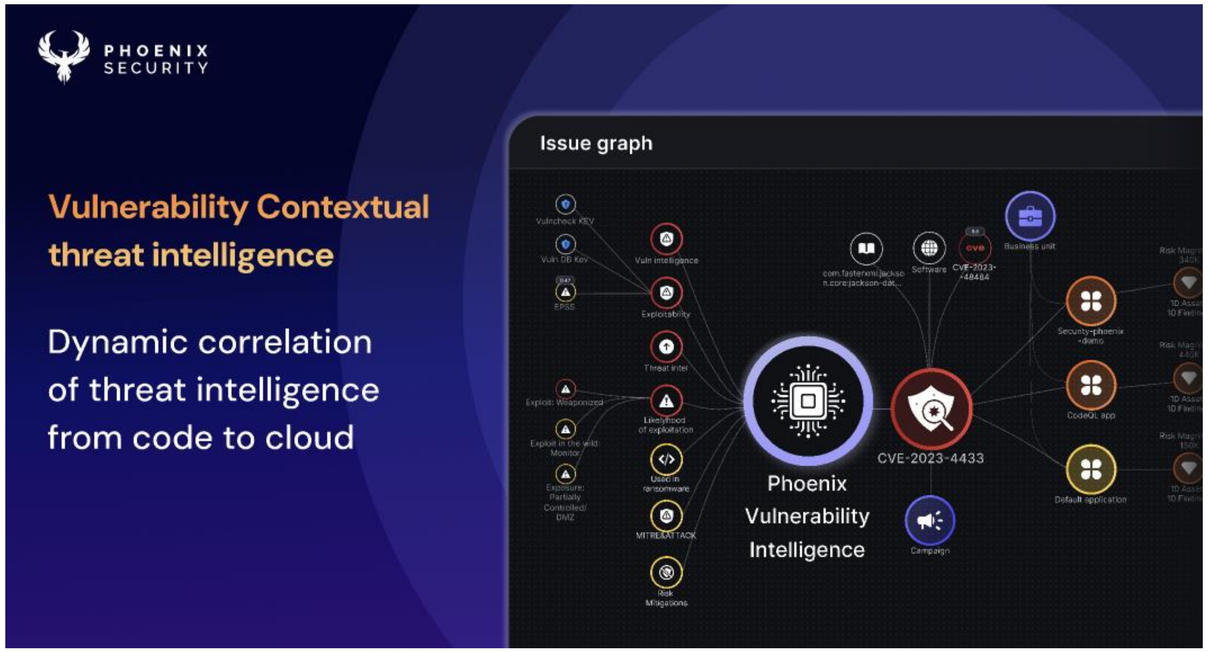
PHOENIX SECURITY

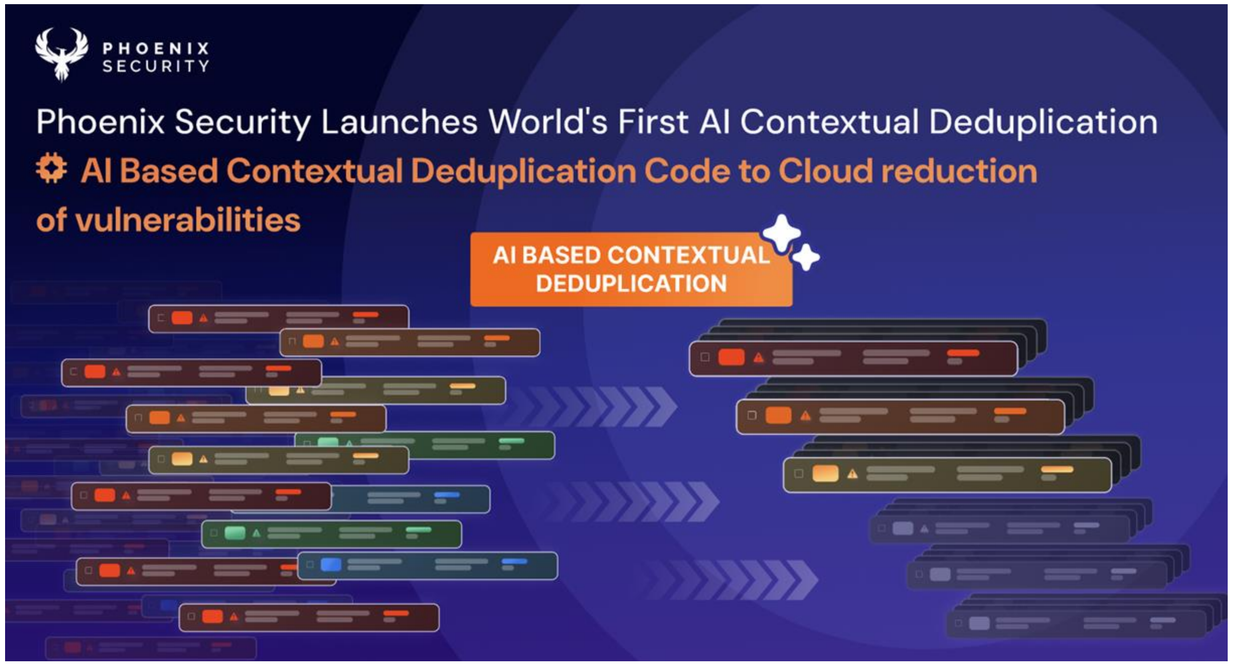
Phoenix Security Launches World's First AI Contextual Deduplication

AI Based Contextual Deduplication Code to Cloud reduction of vulnerabilities



Upcoming New Features





Building resilient application and cloud security programs

NEW EDITION

PHOENIX SECURITY

BUILDING RESILIENT APPLICATION AND CLOUD SECURITY PROGRAMS

Author
Francesco Cipollone
CEO & Founder
Phoenix Security

Timo Pagel
DevSecOps
(DSOMM)

Kane Narrraway
Security @ CANVA

OMO OSAGIEDE
Security Architect

Chris Hughes
CEO & Founder
ACQUIA

Sam Moore
Vulnerability Management @ TMOBILE

Anuprita Patankar
Product Security @ Ecommerce Company

Chintan Gurjar
Vulnerability Management @ M&S

Cyber Risk Defender Club

PHOENIX SECURITY

CYBER RISK DEFENDERS CLUB

Author
Francesco Cipollone
CEO & Founder
Phoenix Security

Timo Pagel
DevSecOps
(DSOMM)

Kane
Narrraway
Security @
CANVA

OMO
OSAGIEDE
Security
Architect

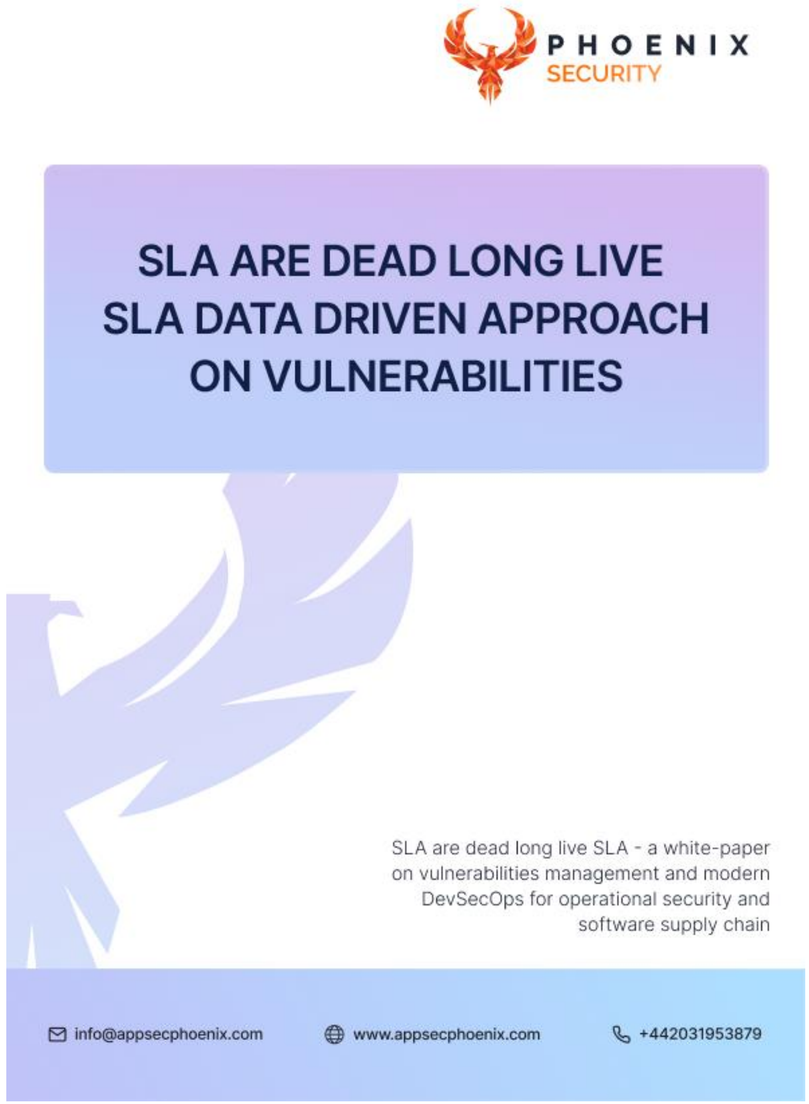
Chris Hughes
CEO & Founder
ACQUIA

Sam Moore
Vulnerability
Management @
TMOBILE

Anuprita
Patankar
Product
Security @
Ecommerce
Company

Chintan
Gurjar
Vulnerability
Management
@ M&S

New Book on metrics that matters



Where can you find more

We have whitepapers on vulnerability management prioritization

PHOENIX SECURITY

APPLICATION & CLOUD SECURITY PROGRAM

PHOENIX SECURITY

VULNERABILITY MANAGEMENT AT SCALE AND THE POWER OF CONTEXT BASED PRIORITIZATION

Cyber Security & Cloud Podcast

By Francesco Cipollone

#CSCP

www.cybercloudpodcast.com

@podcast_cyber

@FrankSEC42

www.cybercloudpodcast.com

Sponsored By

PHOENIX SECURITY