Threat intelligence and attack surface

Product Security & Modern approach on software security and the evolution of attack surface

PHOENIX SECURITY

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

Warning revelation ahead

Warning

About Francesco

Francesco Cipollone

CEO & Co-Founder Security Phoenix, Board CSA UK

I'm a appsec passionate and have been a CISO Advisor, Cybersecurity Cloud Expert.
Speaker, Researcher and Board of Cloud security Alliance UK.
Currently we are working on interesting problem on how to link Application, Security and

@FrankSec42 | Fracipo Linkein | Email | Website | Articles | NSC42 LinkedIn

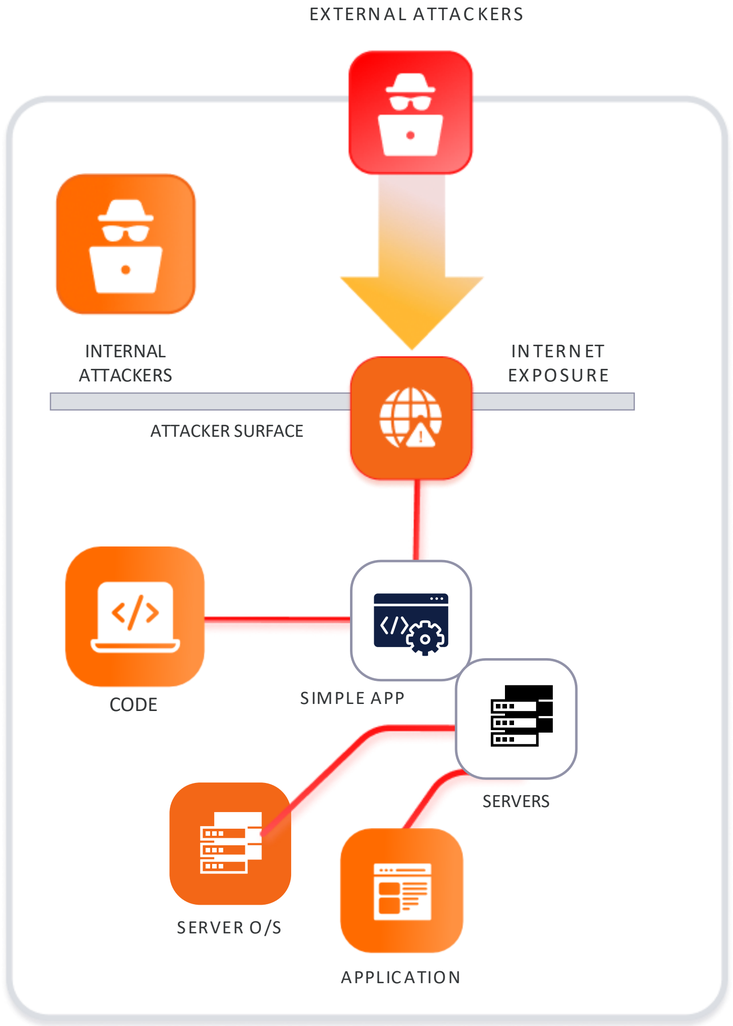
You can argue with people, but you can't argue with data

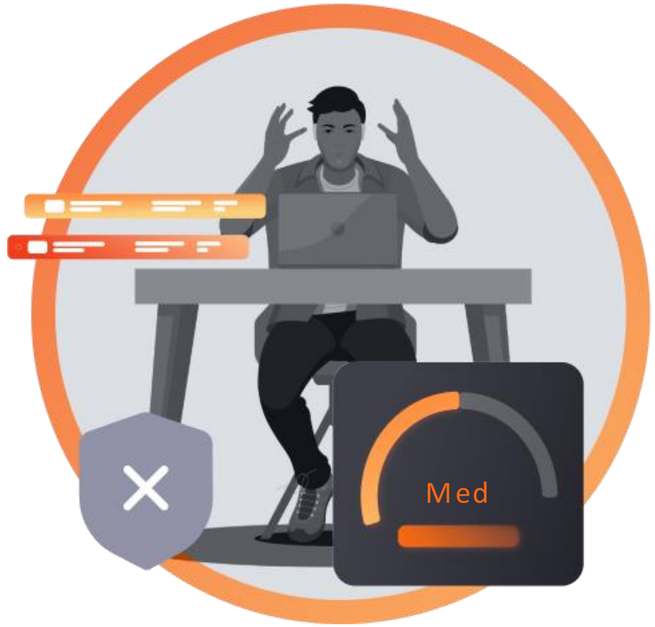
Data driven approach can help making compelling arguments

Agenda

- Intro & Context
- Current Scenario : 2015 to today
  - Vulnerability growth
  - Time to remediate
  - How we addressing today
- Driving to a Higher Maturity
  - Devops and Devsecops
  - Identify what to fix first
  - Demystify: attribution, lineage, reachability, attack path
- Data Driven approach: Vendor with highest exploitation
  - Exploit in the wild
  - Ransomware/ Zero Day
- Anatomy of vulnerability: Category and Technical Impact
- Prioritizing with data Data Driven approach supply chain
  - Reduction using intelligence & Context
  - Risk driven approach
- Conclusion & Q&A

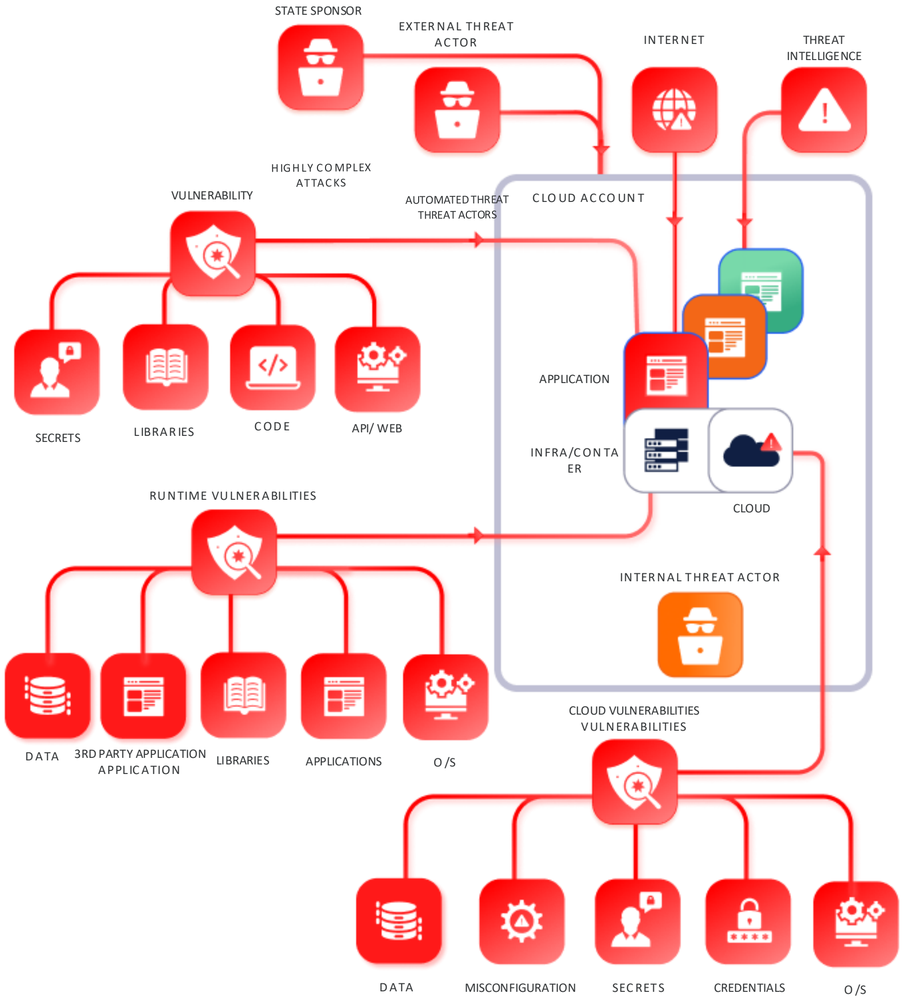
Context: In 2015 we had fewer security tools, digital software supply chain was simpler, and the attack surface was smaller, so finding fixes was trivial

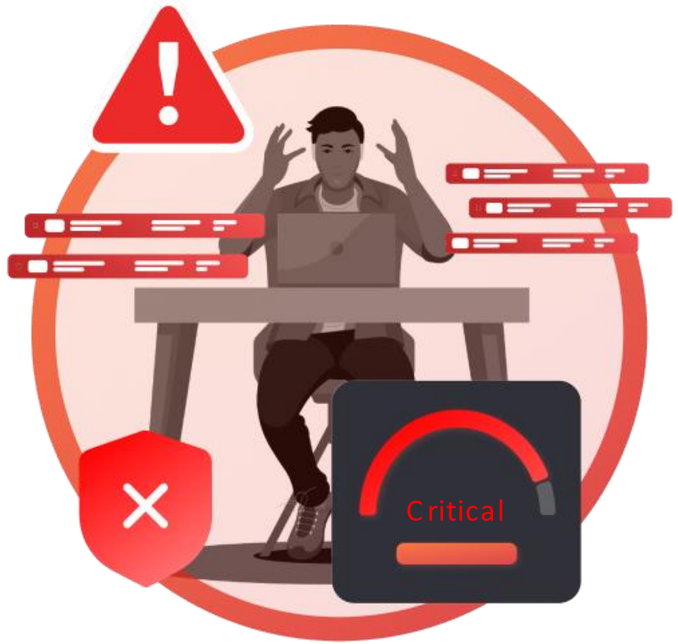




- **Total Number of CVEs:** 15 K (now 222 K+)
- **Few scanners / limited attack surface**
- **Monolithic software deployed on premises**

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: 220 K (vs 6.7k in 2015) while team size has not increased**
- **Multiple alerts all disconnected, multiple disjointed processes and reports**
- **<u>Larger</u> software attack surface built by multiple teams releasing frequently**

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

#CVE
220,538 **

35% YoY increase

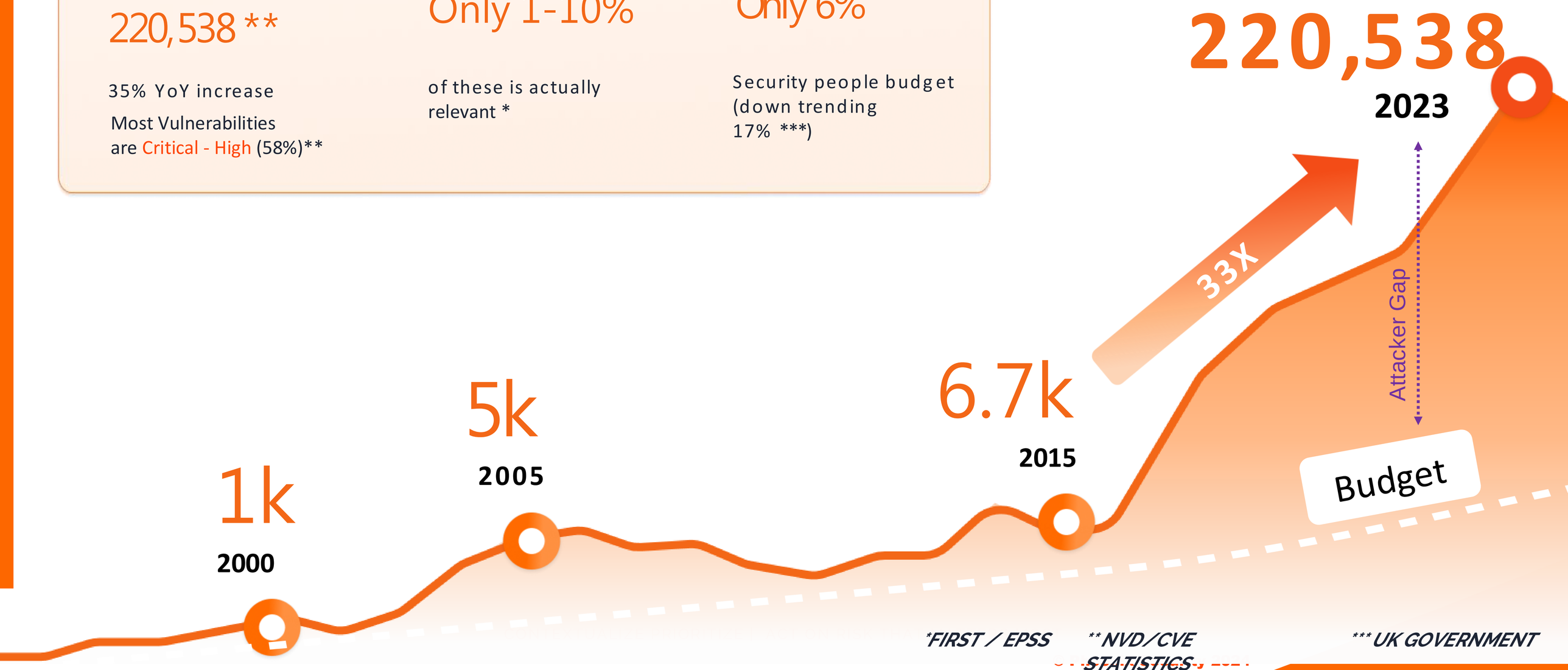
Most Vulnerabilities are Critical - High (58%)**

Only 1-10%

of these is actually relevant *

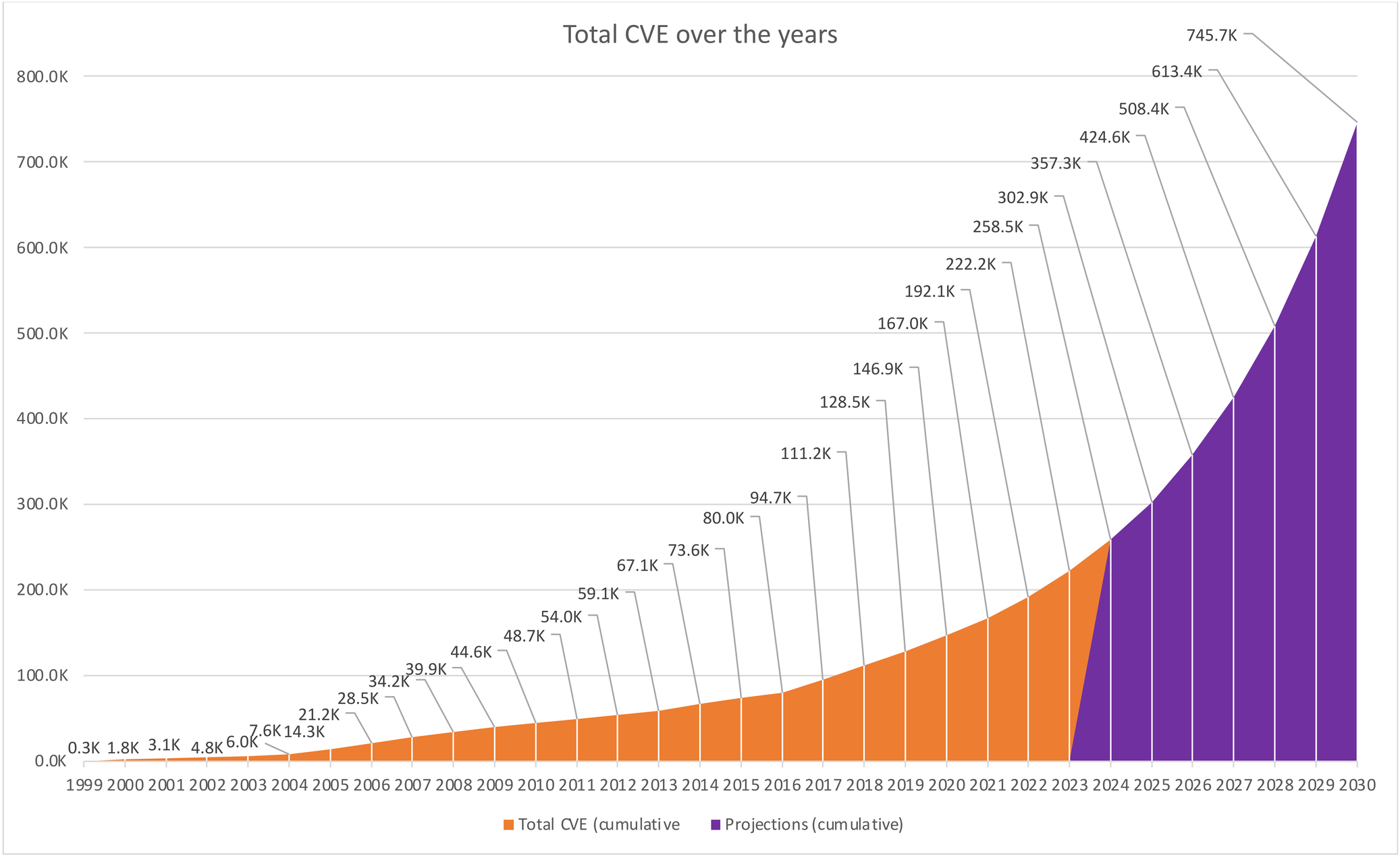
Only 6%

Security people budget (down trending 17% ***)



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

The Race to a Million vulnerabilities...not that far away



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

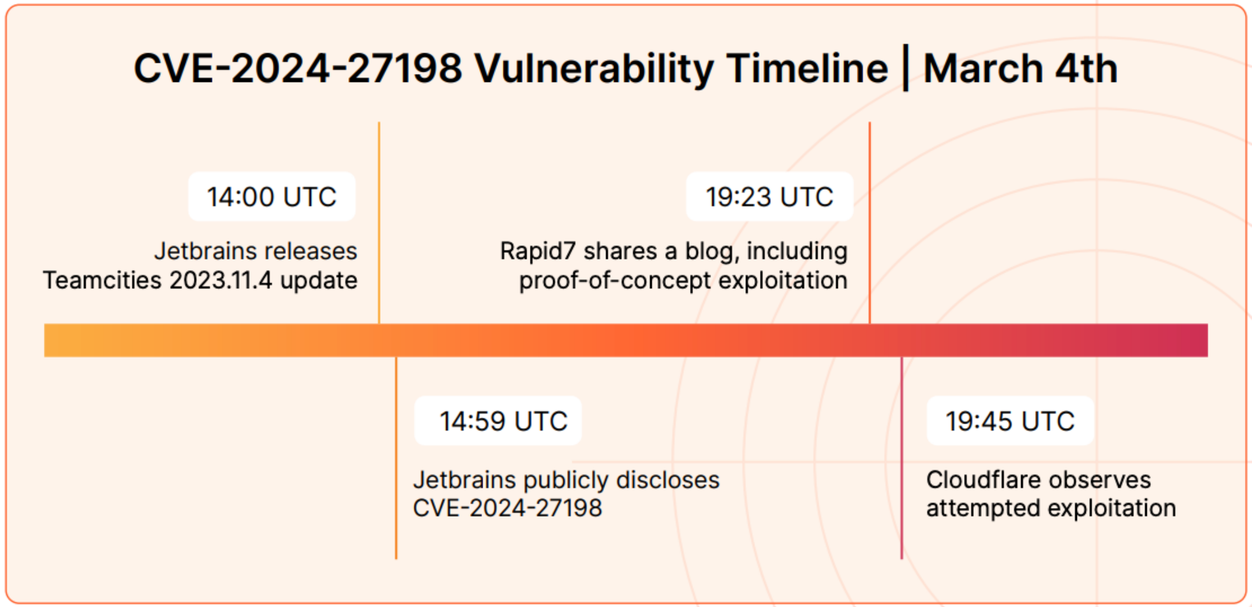
> Data from GitHub reveals that "41% of all code right now is AI generated," Mostaque remarked. More interestingly,
>
> GitHub CTO

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.

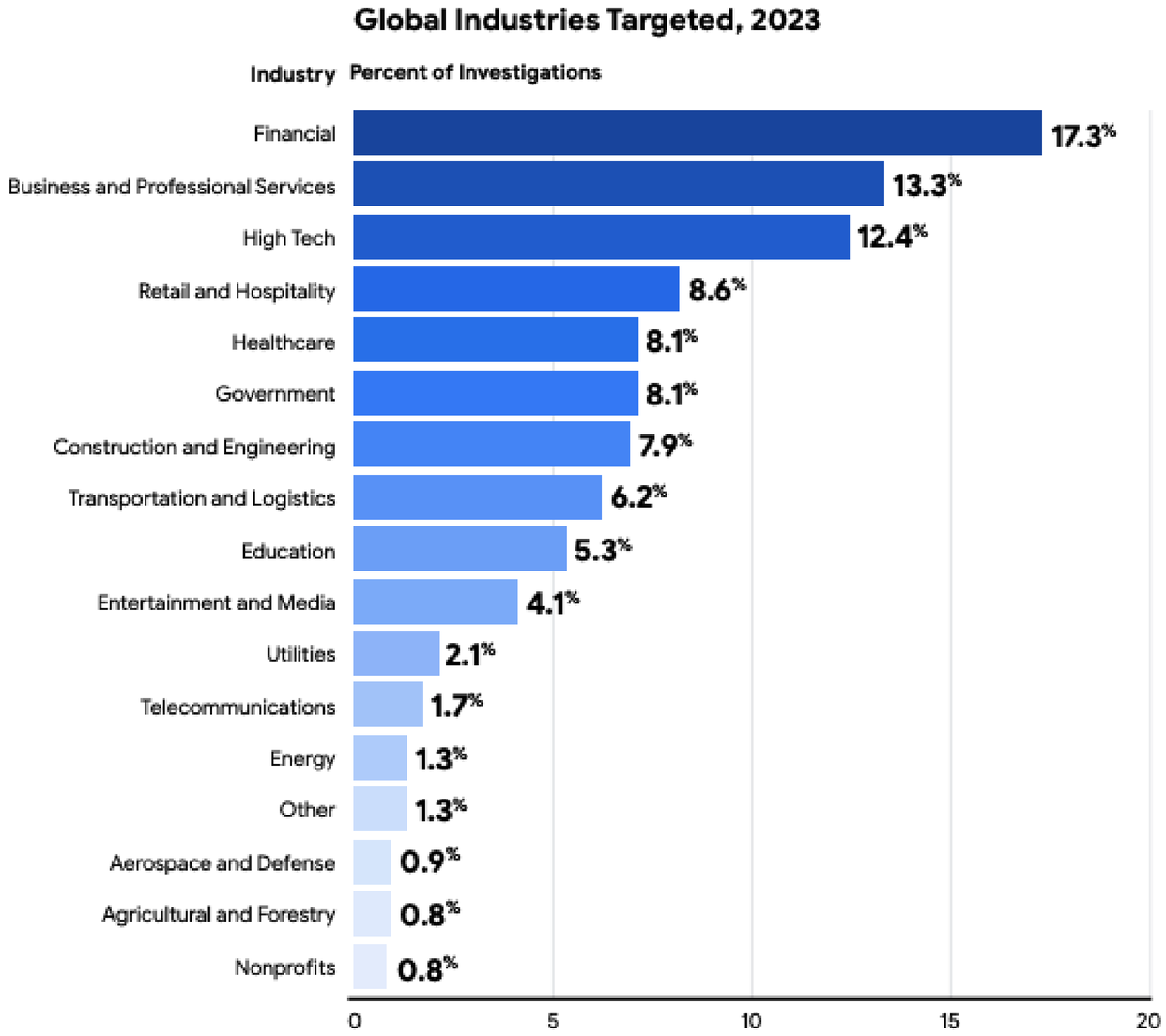


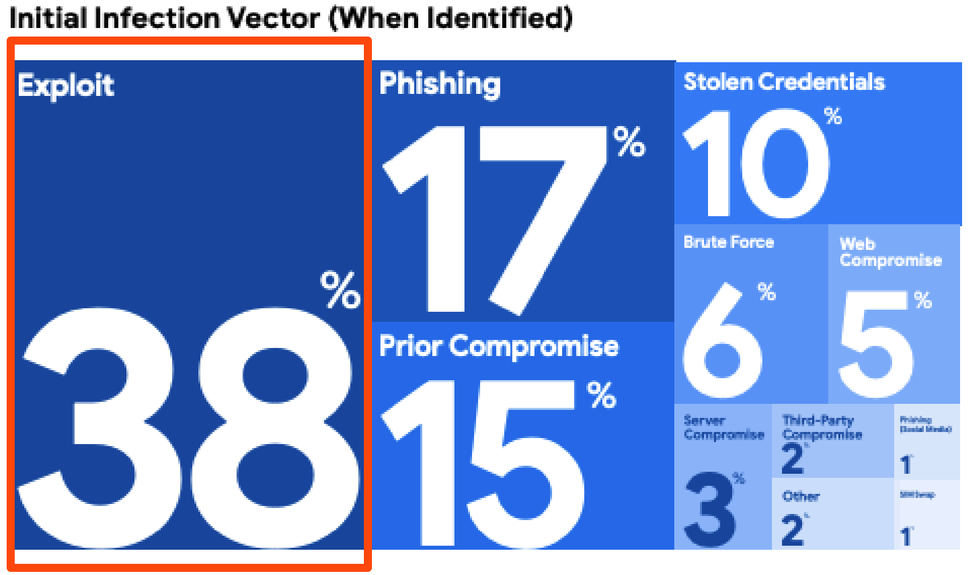
← 3 Minutes** →

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

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

Who is attacking what and where





Reference https://www.mandiant.com/m-trends

Vulnerability Exploits is on the raise

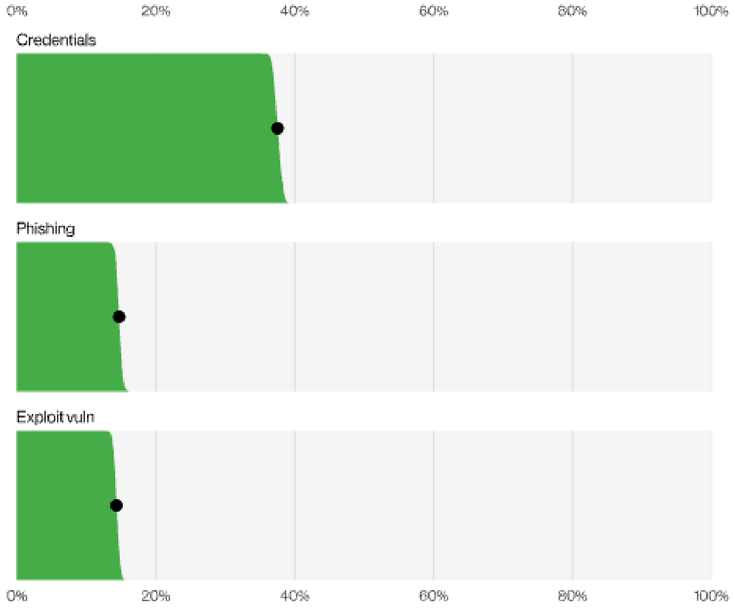
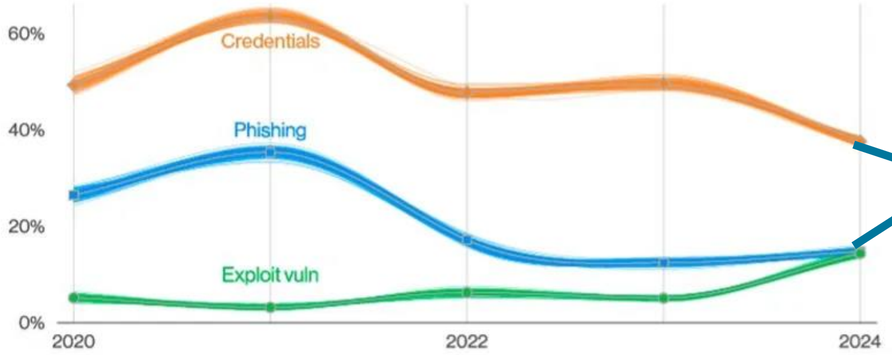
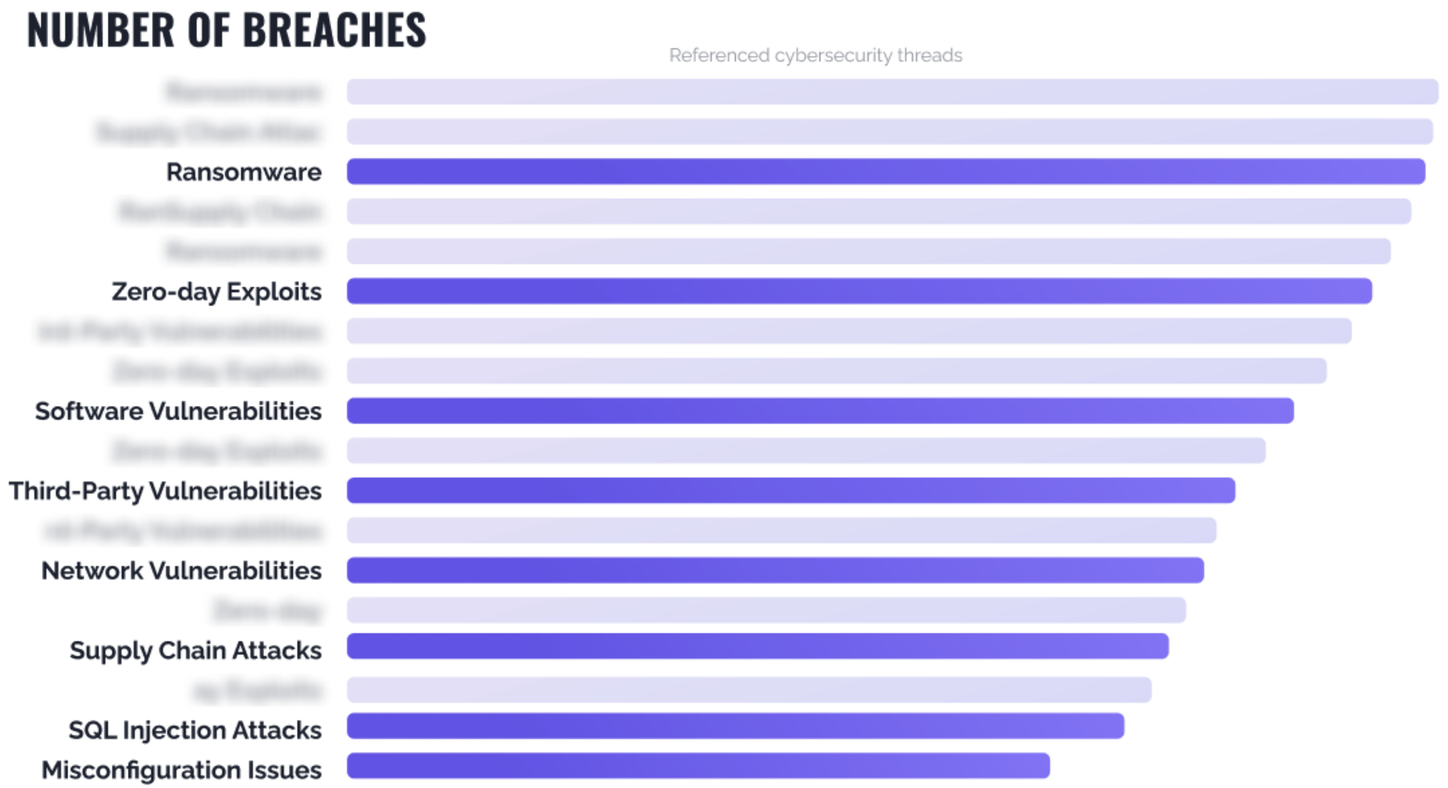


Figure 1. Select ways-in enumerations in non-Error, non-Misuse breaches (n=6,963)

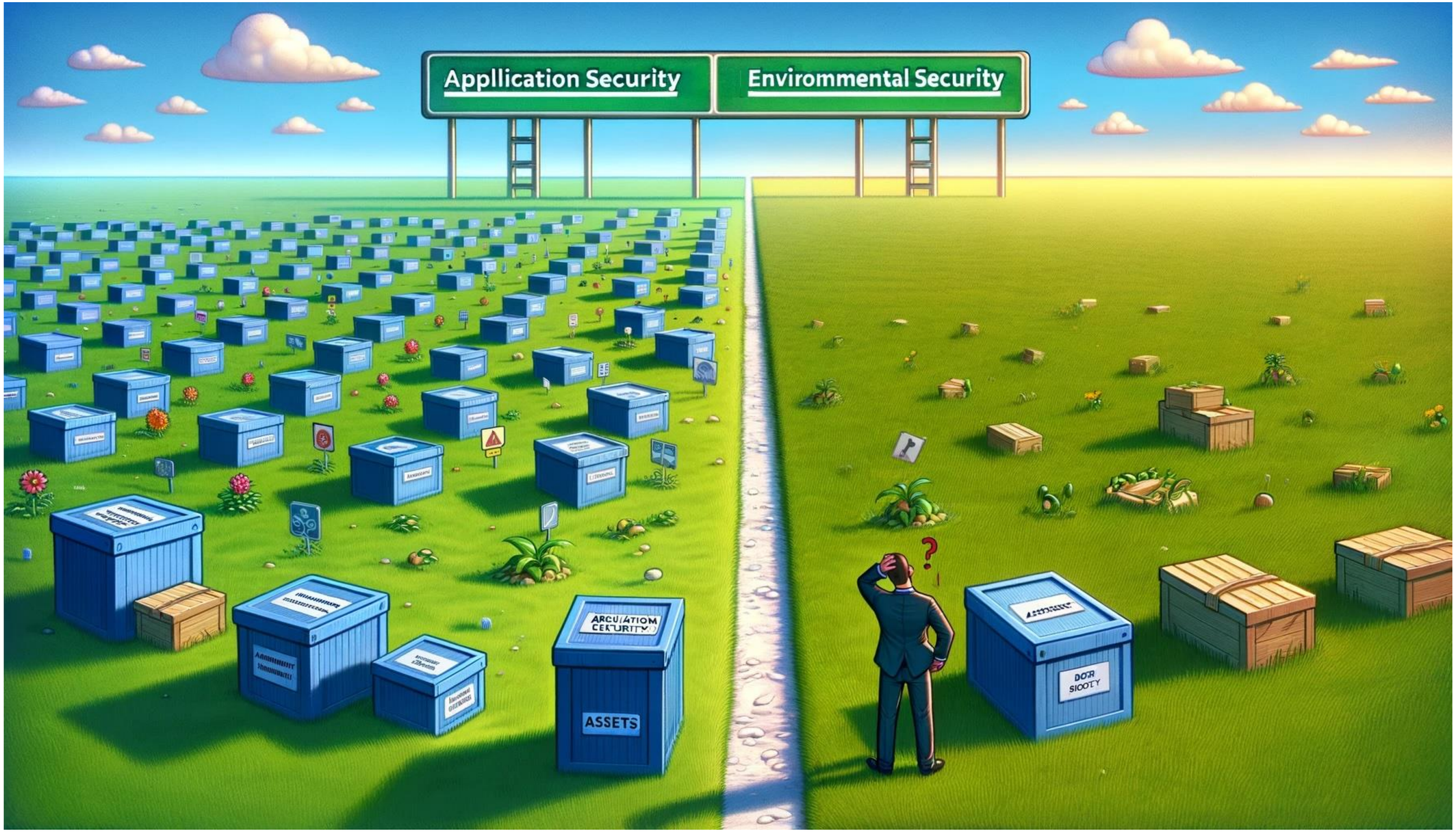




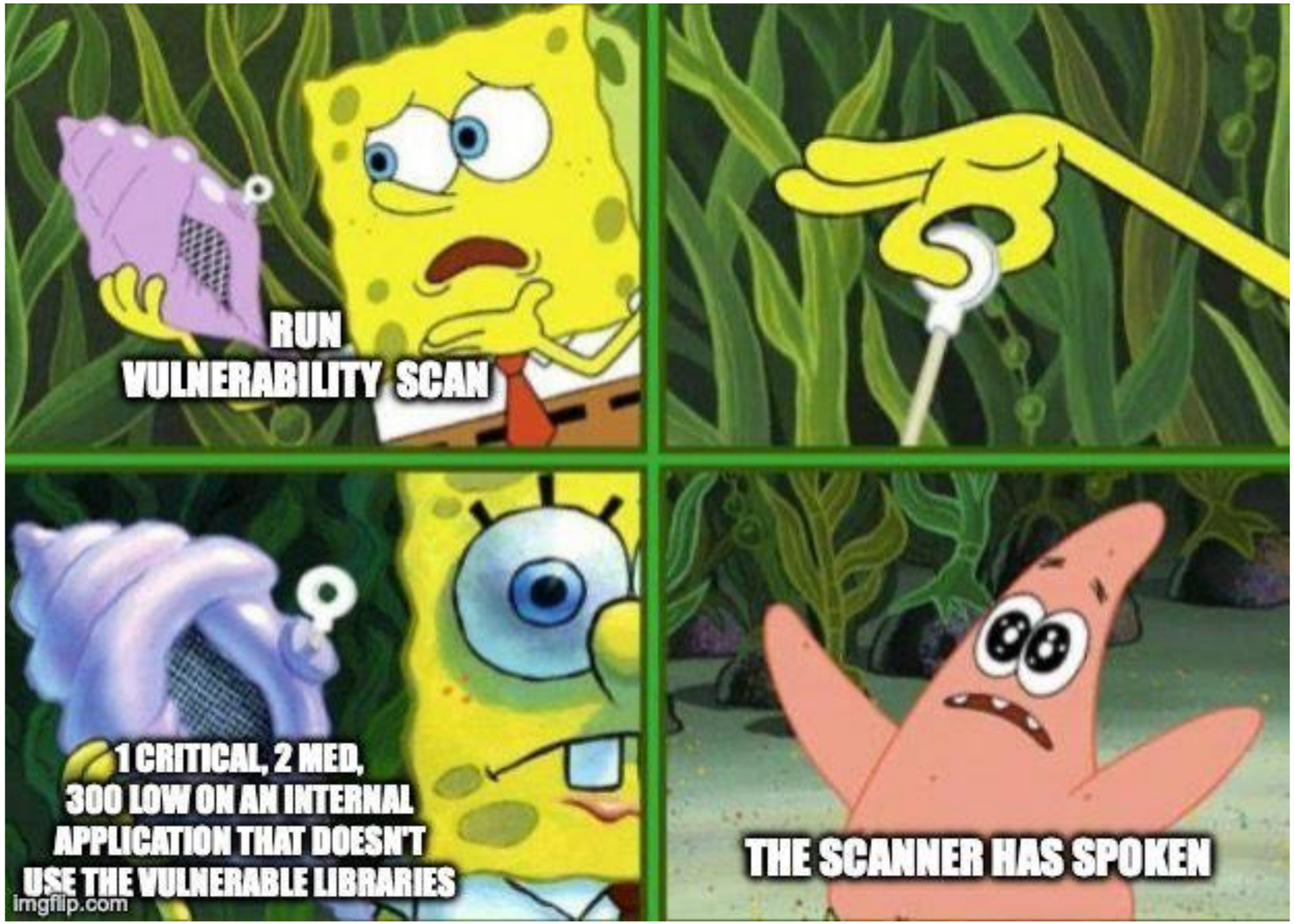
By 2025 the line will cross

Reference DBR 23

Assets and Risk, what are your assets, where is your risk?



How Do we assess now?



The Vulnerability Cycle

Step 1 – Overload Dev

Step 2 – Pray they catch that 1 vulnerability

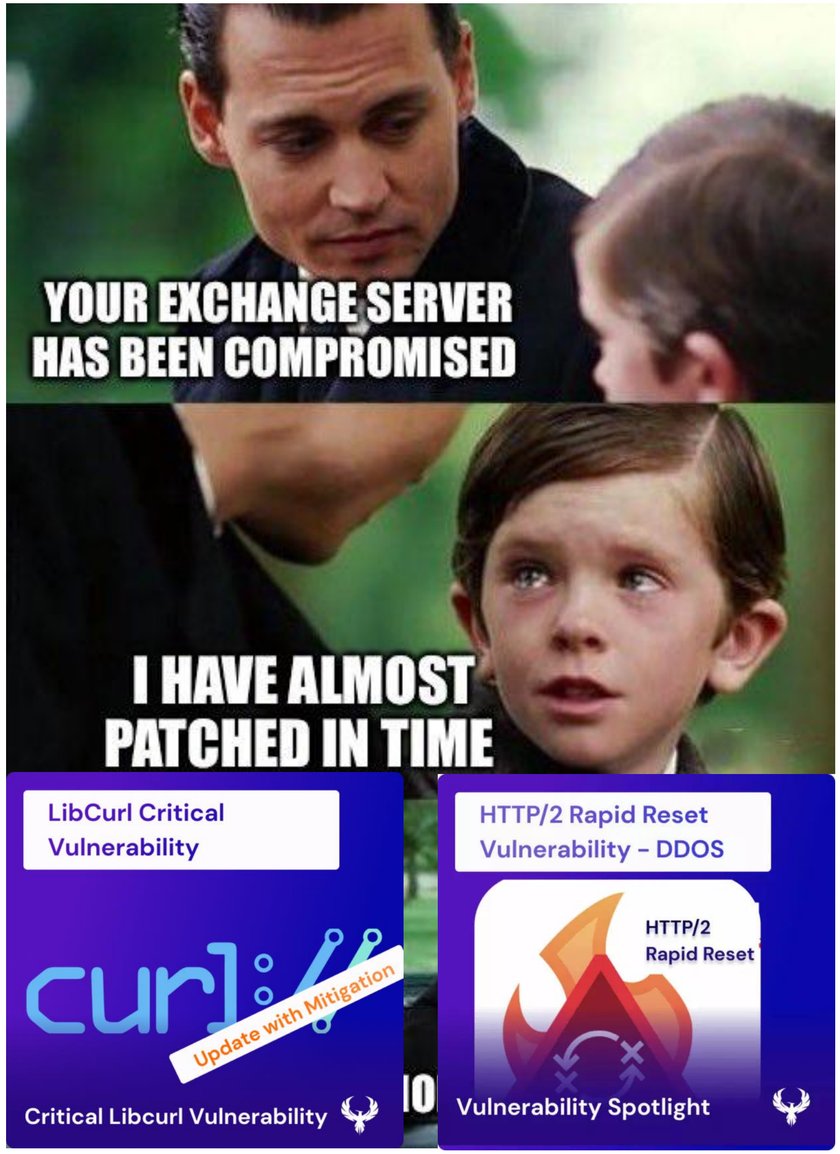
Step 3 – That 1 vulnerability get compromised

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 ask to fix by 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

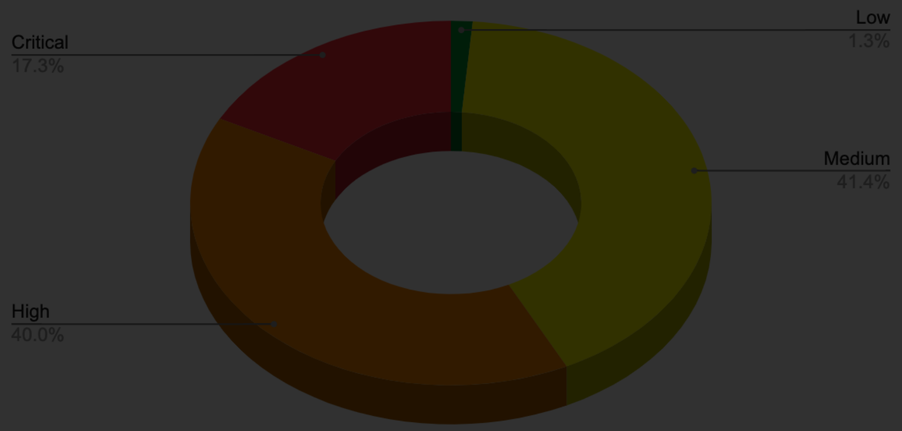
WHO does WHAT where and how IMPORTANT is it

Identify what to fix first IS COMPLEX

MANUAL TRIAGE DOES NOT SCALE

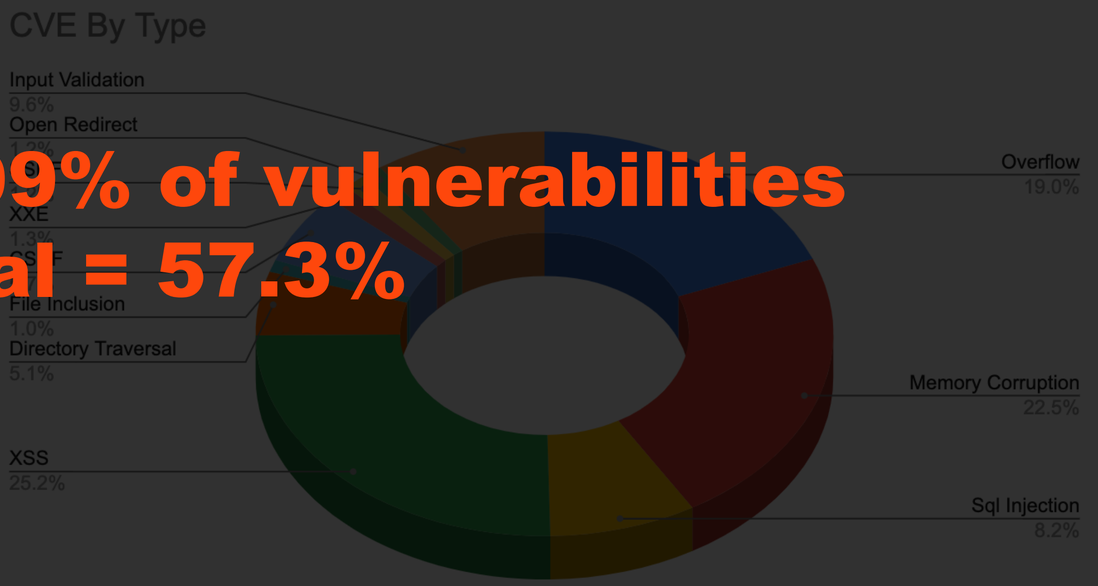
SME	Mid Size Organization
1000 Employees	3100 Employees
100 Dev 2 Security 1:50 Security to Dev	1000 Dev 5 Security 1:200 Security to Dev
48 min per team	**10<min per team**
9h to analyse a vuln	9h to analyse & triage a vuln

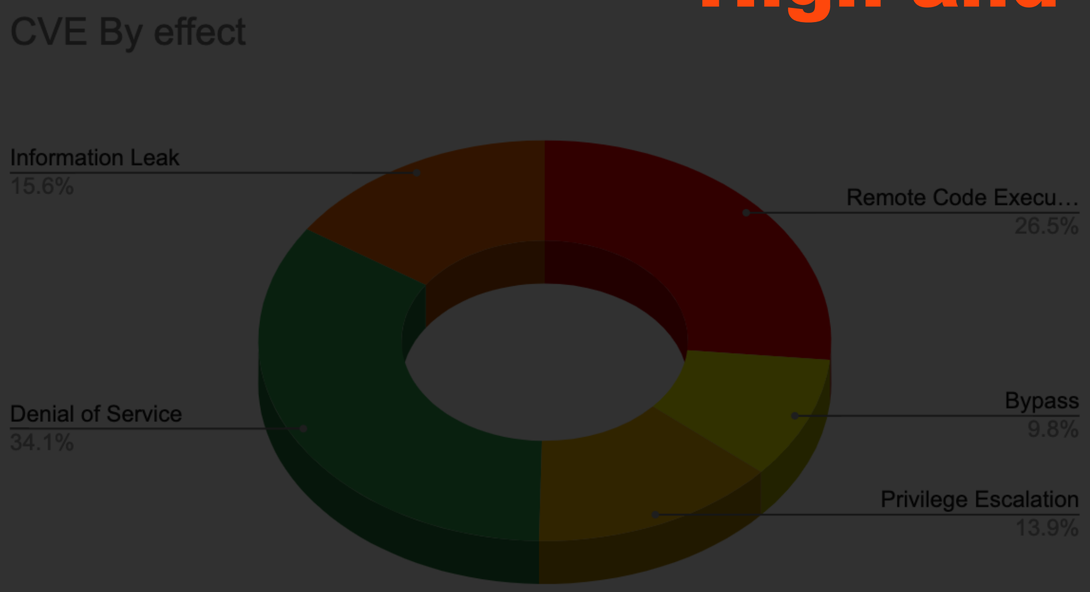
Fix By CVE vs FIX by Criticality



PCI DSS Fix Medium + = 99% of vulnerabilities

High and Critical = 57.3%

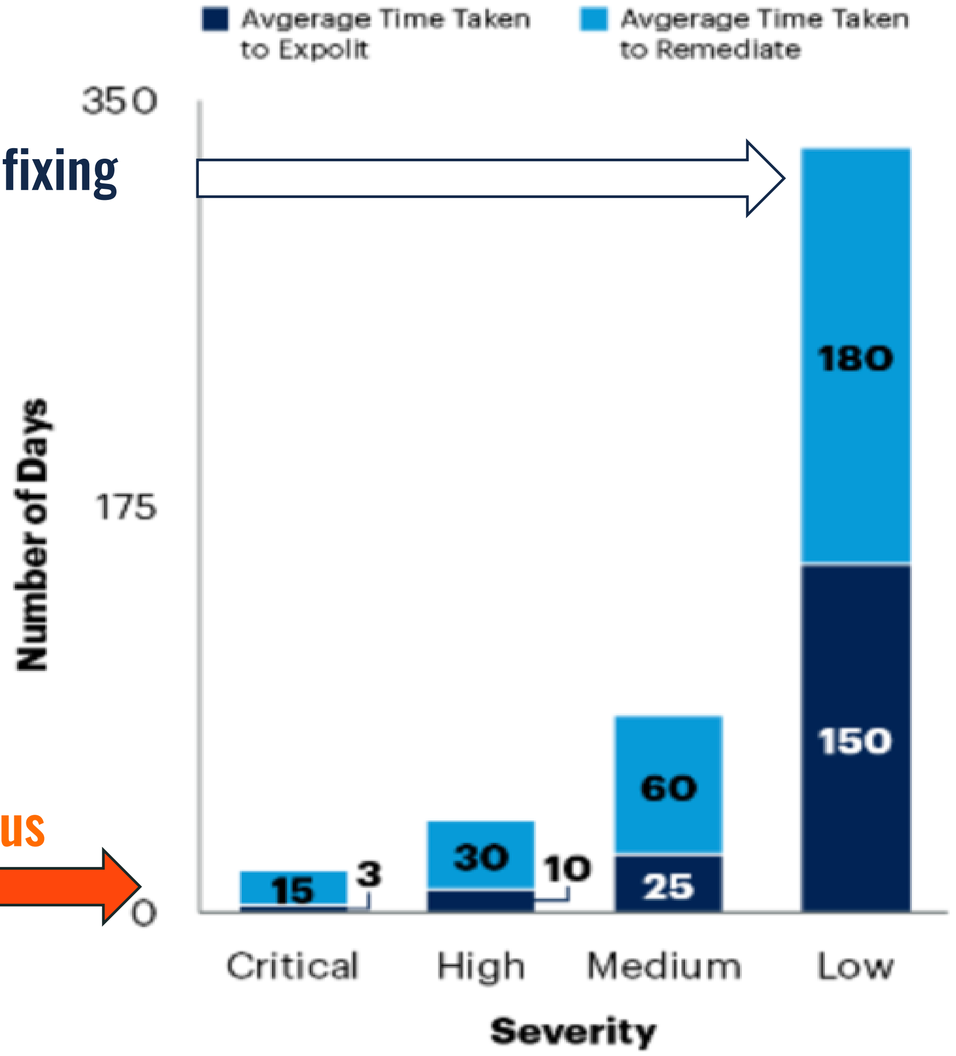




WE ARE FIXING SLOWER THAN ATTACKERS

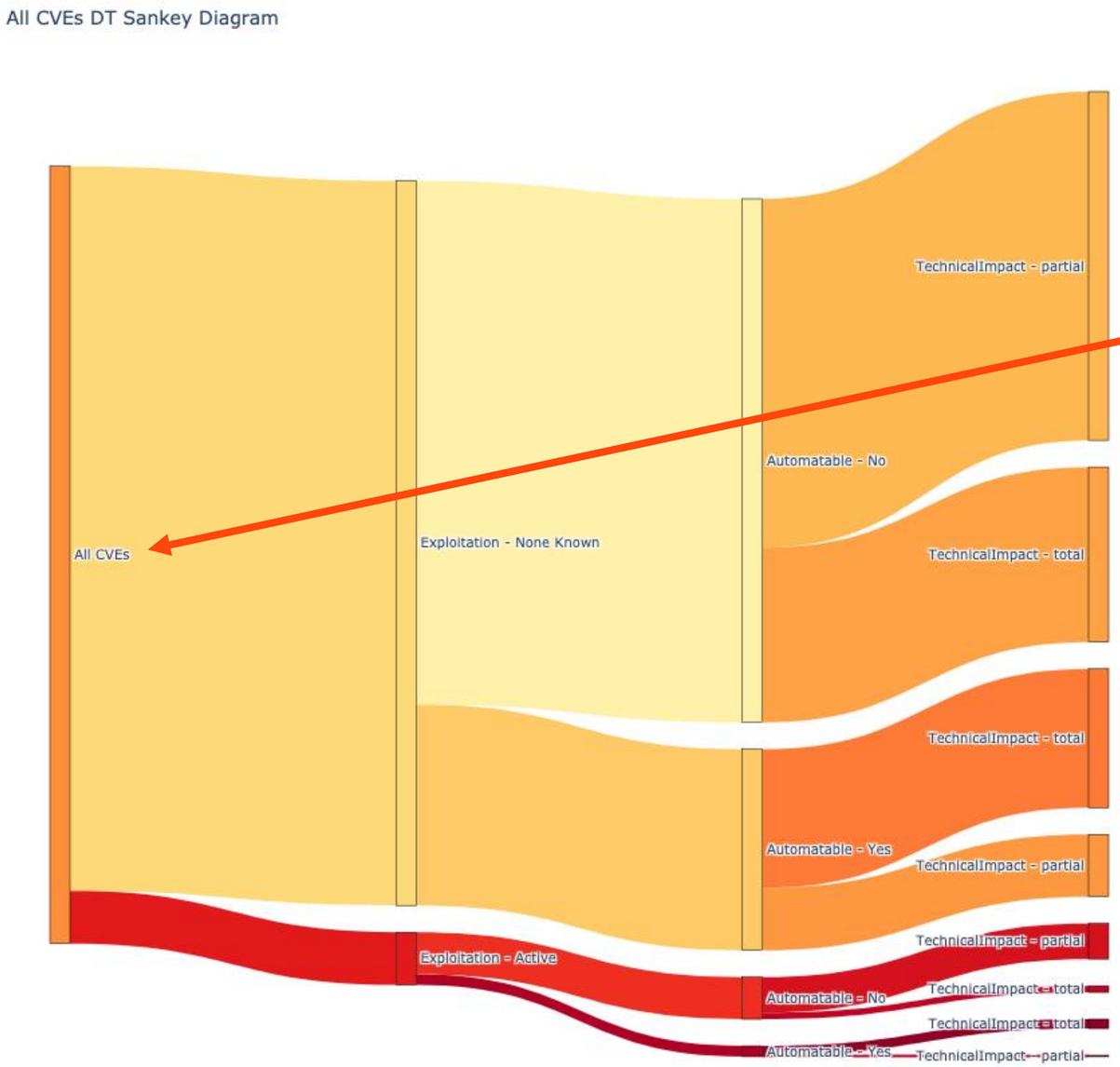
How fast are you fixing

Where you should focus



Source: Gartner
760501_C

Current Flow of vulnerabilities only 1% are exploitable



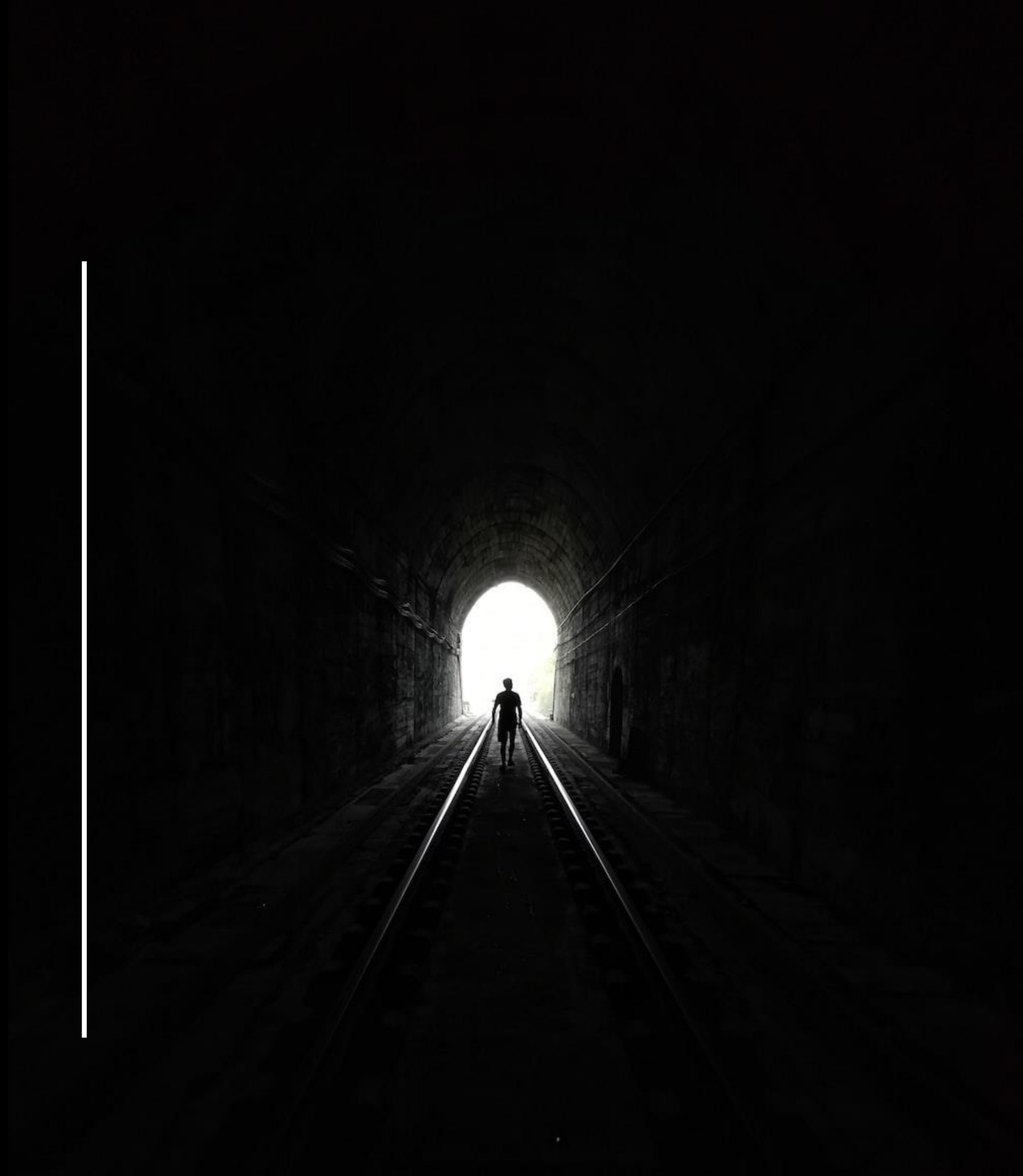
Current Focus

Really important to focus on

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



How do we fix without burning out?

Part 1 Attribute the right vulnerability to the right team in the right Context

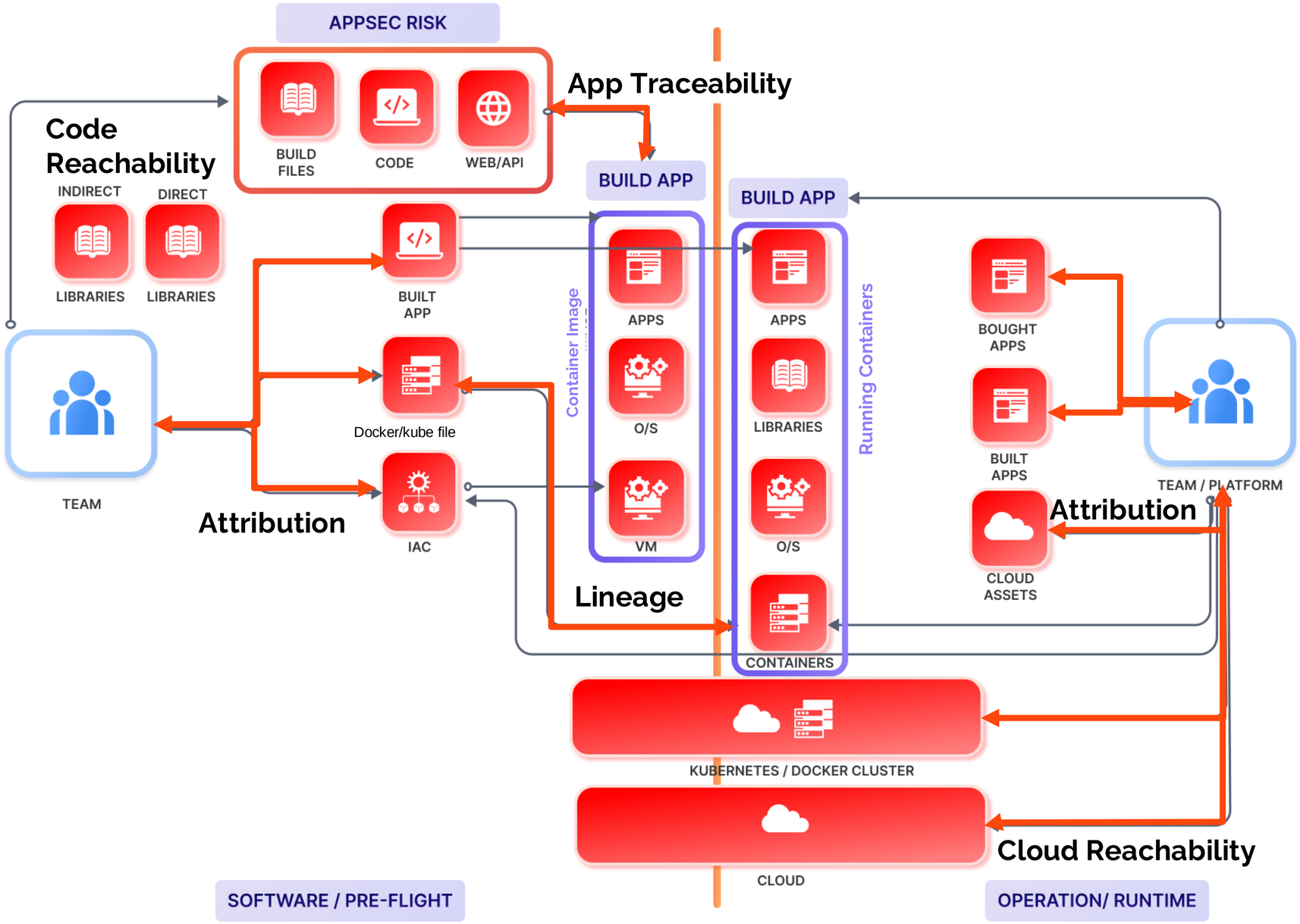
Part 2 Understand which vulnerability needs to be addressed first

Part 3 Automate Triage and remediation with contextual communication

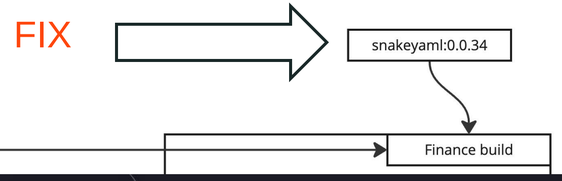
Part 1 - Attributing the right vulnerability with right context

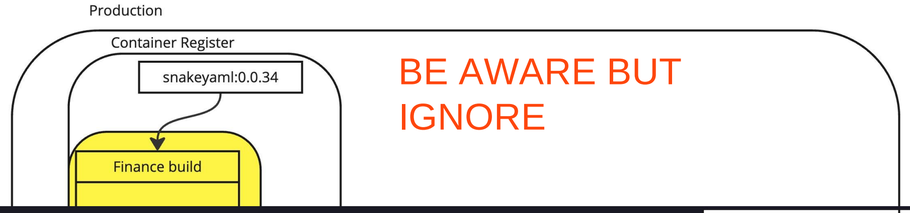
Phoenix correlates, contextualizes and deduplicates by linking together assets using 4 dimensions

- Attribution
- Lineage
- Traceability
- Code/Cloud Reachability



Real Case Scenario : Deduplicating Contextually Code and Libraries





BE AWARE BUT IGNORE

Where

CVE-2022-1471 * Numb

SCA Library pre

Issue is higher b
application is be
container that is
multiple times

PHOENIX SECURITY

- Dashboard
- Risk Explorer
- Assets
- External Dependencies
- Security
- Vulnerabilities
- Assessment Imports
- Teams
- Automation
- Integrations
- Settings

Vulnerabilities

Vulnerabilities | Findings | Group by Location

Finding Status: Open | Closed | All

Search: CVE-2022-1471 Clear All

Filters 1

Application / Environment: Select Application or Environment

Team: Finance-Fullstack Clear all

2 Results

Export Findings

Risk	Asset/Location	Name	Type	CVSS / Severity	Discovery Days	Remediation Days	Exploitability (EPSS)	Risk Exception	Create Ticket / Ticket Status	Source
985	.../ container-finance:0.0.34 .../financeapp/lib/snakeyaml-1.30.jarLorg.yaml:snakeyaml:1.3.0	org.yaml:s...	Ignore	9.8	9	N/A	2.1%		-	
985	.../ finance-backend/prod org.yaml:snakeyaml	Arbitrary ...	Fix	6.6	15	N/A	2.1%			

Items per page: 100 1 – 2 of 2

Part 1 (cont) - Communicating with the right context

Shift Everywhere Connect business Security and Development

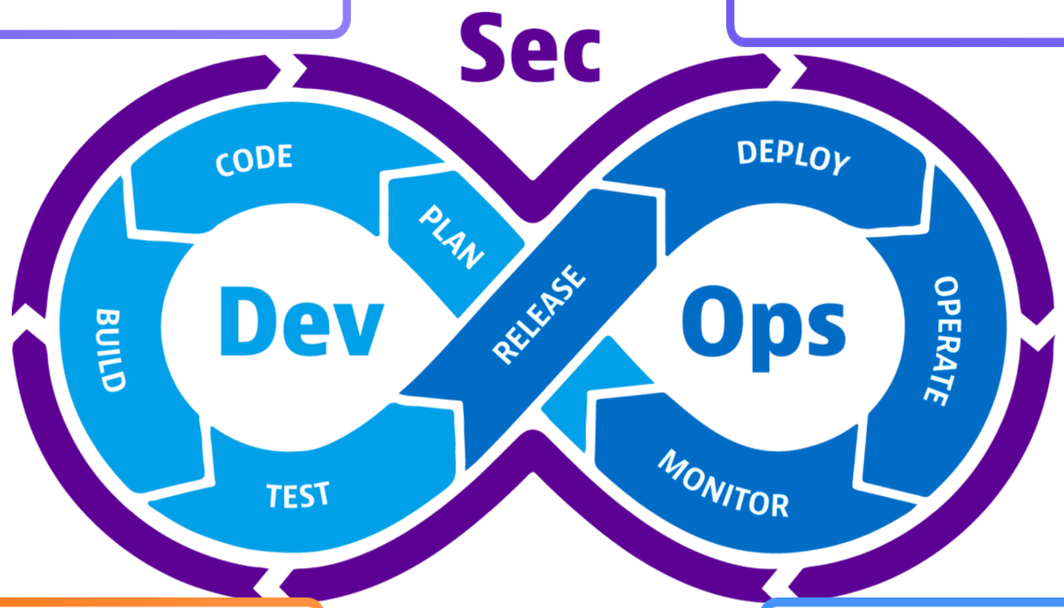
ISC2 CHAPTER LONDON

SHIFT DOWN (Business/SecOps)

- AGREEING RISK BASED TARGETS/ APPETITE
- BUSINESS IMPACT ASSESSMENT
- TRANSLATING RISK BASED PROFILES INTO ACTIONS FOR DEVELOPERS

SHIFT UP (Business/GRC)

- RISK BASED REPORTING
- BUSINESS IMPACT ASSESSMENT
- PRIORITISING, AGGREGATING, COORDINATING RESOLUTION



SHIFT LEFT (DevOps/DevSecOps)

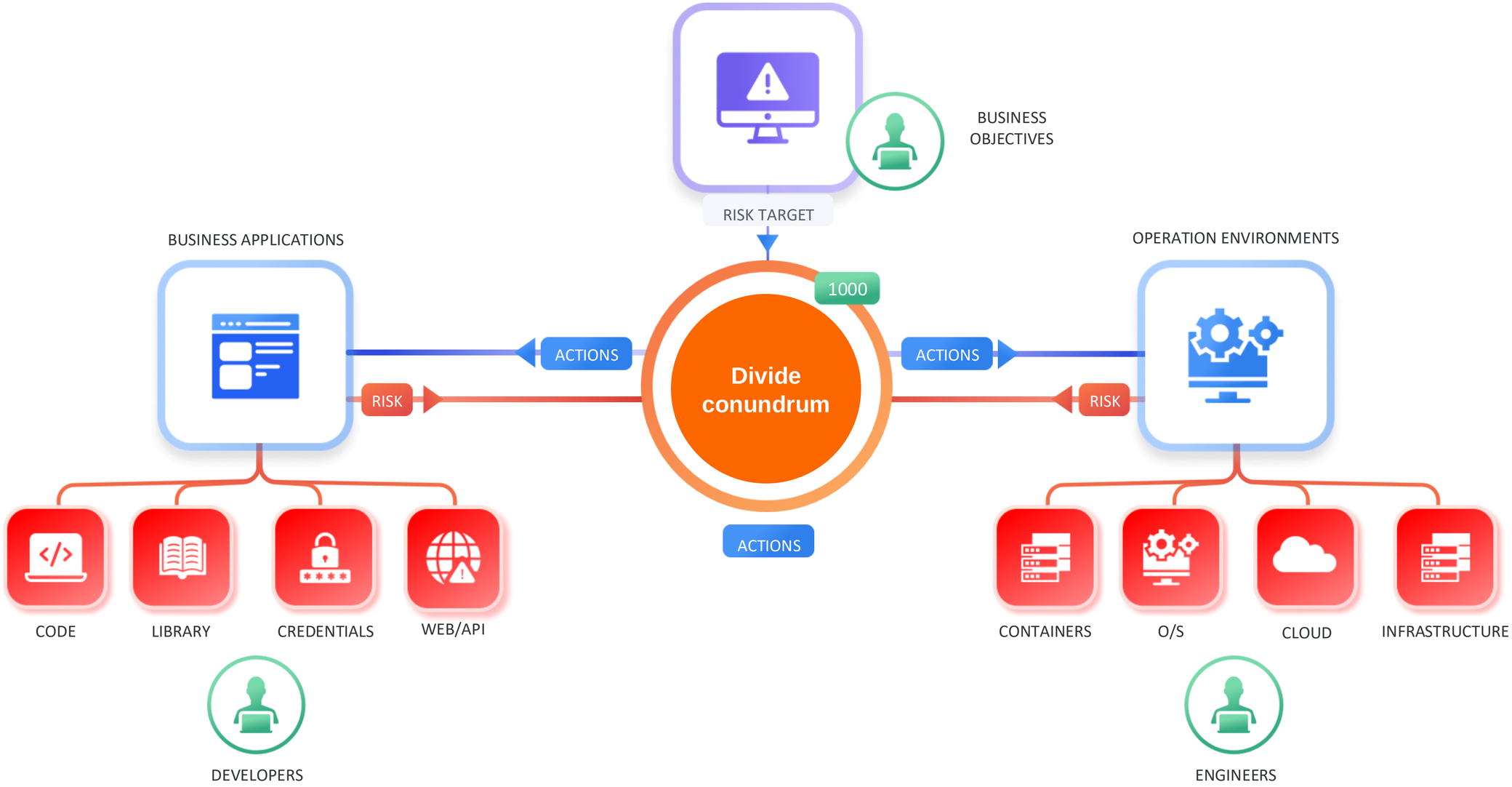
- TESTING CODE AS EARLY AS POSSIBLE
- INTEGRATING CI/CD CHECKS FOR CODE
- THREAT MODELLING, SECURITY BY DESIGN

SHIFT RIGHT (Operation Security)

- O/S TESTING, IMAGE TESTING
- PEN-TESTING, BLACK/WHITE BOX TESTING
- CLOUD MISCONFIGURATION

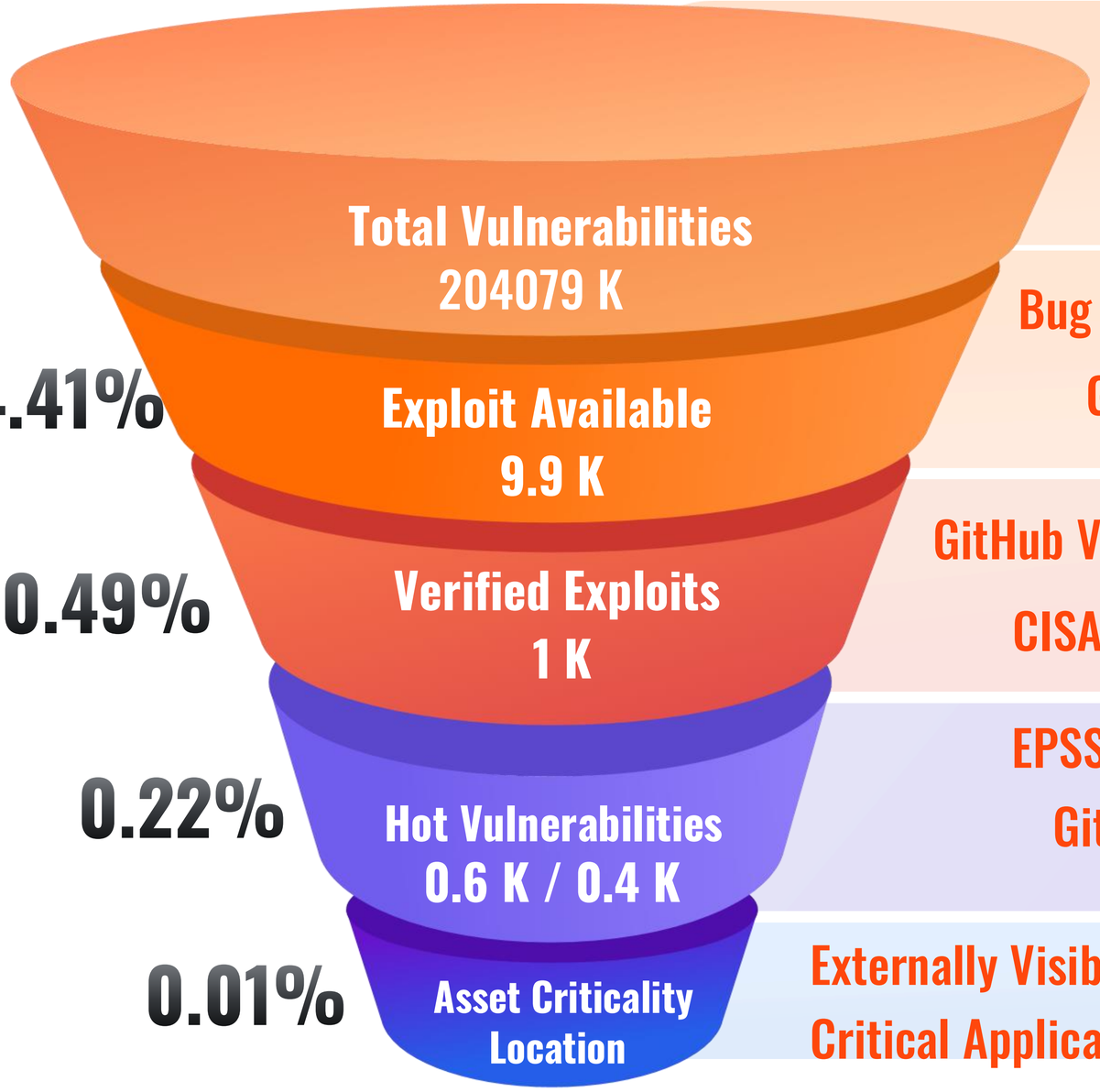
From Number of Vulnerabilities to risk objectives

Drive Risk down, Connect left to right



Part 2 – Which Vulnerability needs to be addressed first

Not all the vulnerabilities require equal attention



4.41%

0.49%

0.22%

0.01%

Bug Bounty Popularity (active 17K) 8.33%

GitHub Exploit (9.9K) 4.41%

GitHub Verified Exploits (0.93K) 0.47%

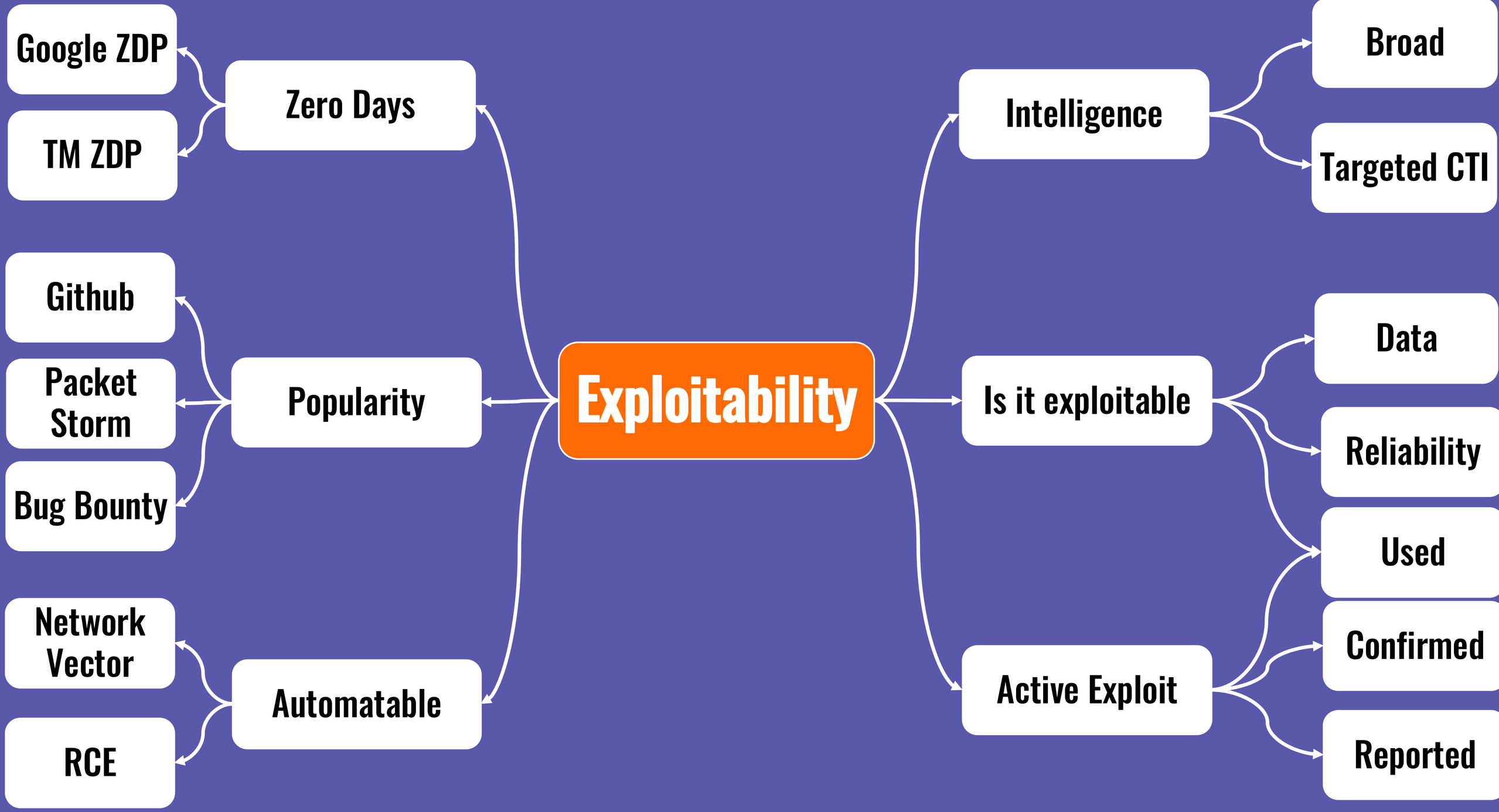
CISA KEV (1K) 0.49%

EPSS > 0.7 (688) 0.34%

GitHub Active Exploit (0.40K) 0.22%

Externally Visible (0.14) ? 0.?%

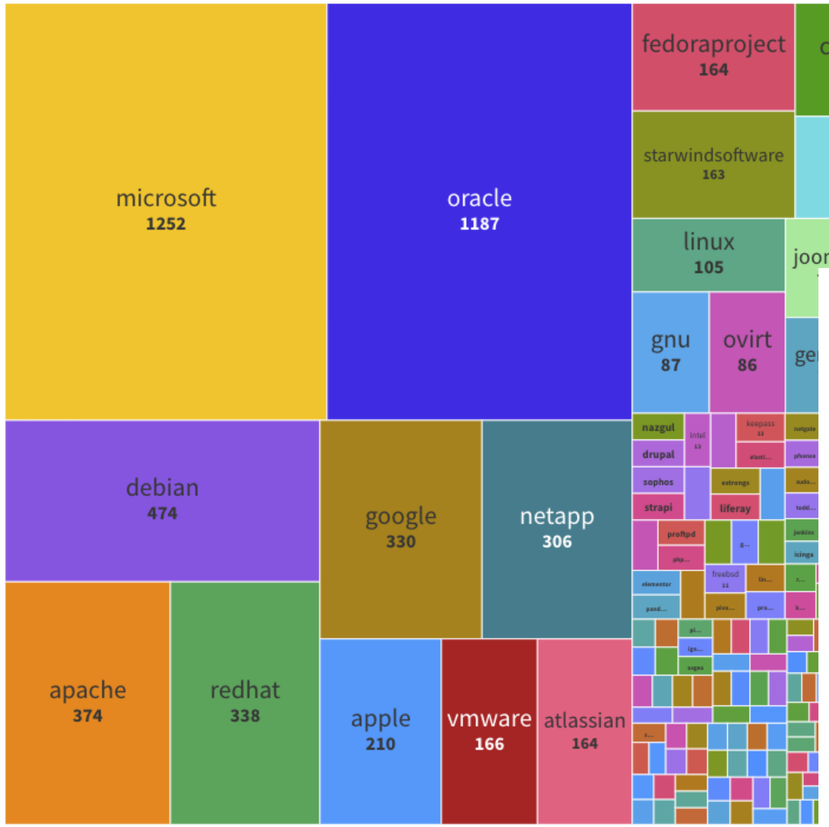
Critical Application


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

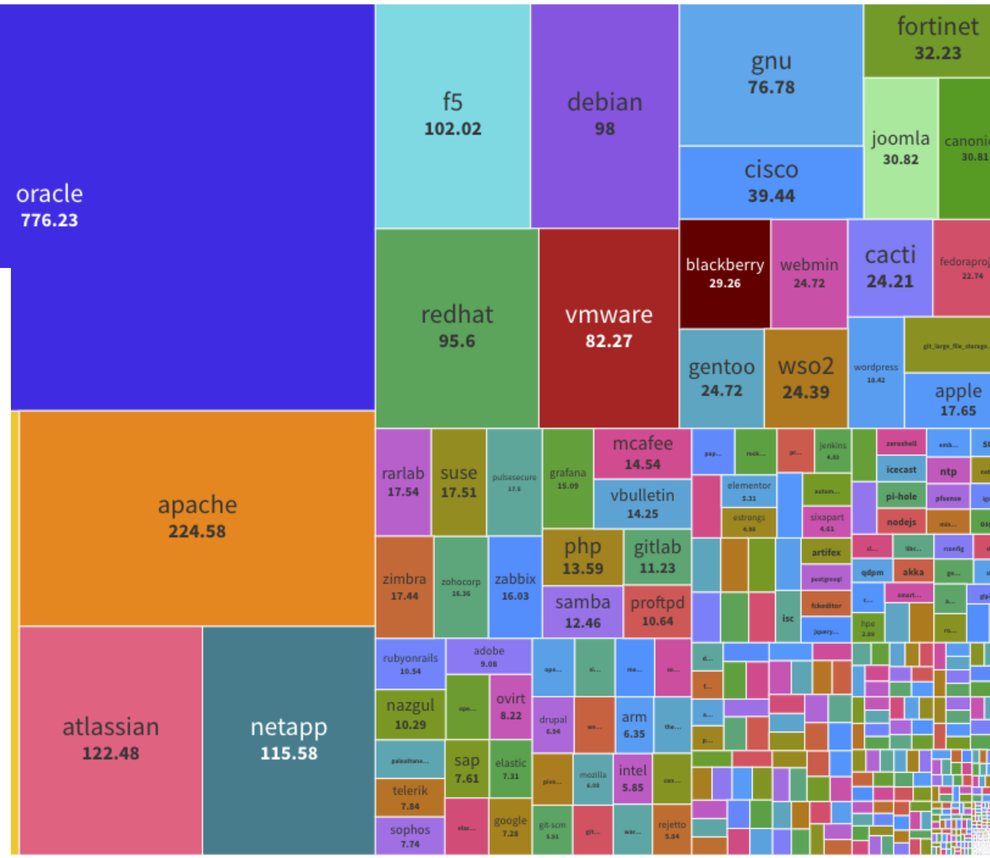
Not all the critical
are critical
Not all the source
are good sources

Phoenix CTI - TOP EXPLOITED VENDOR

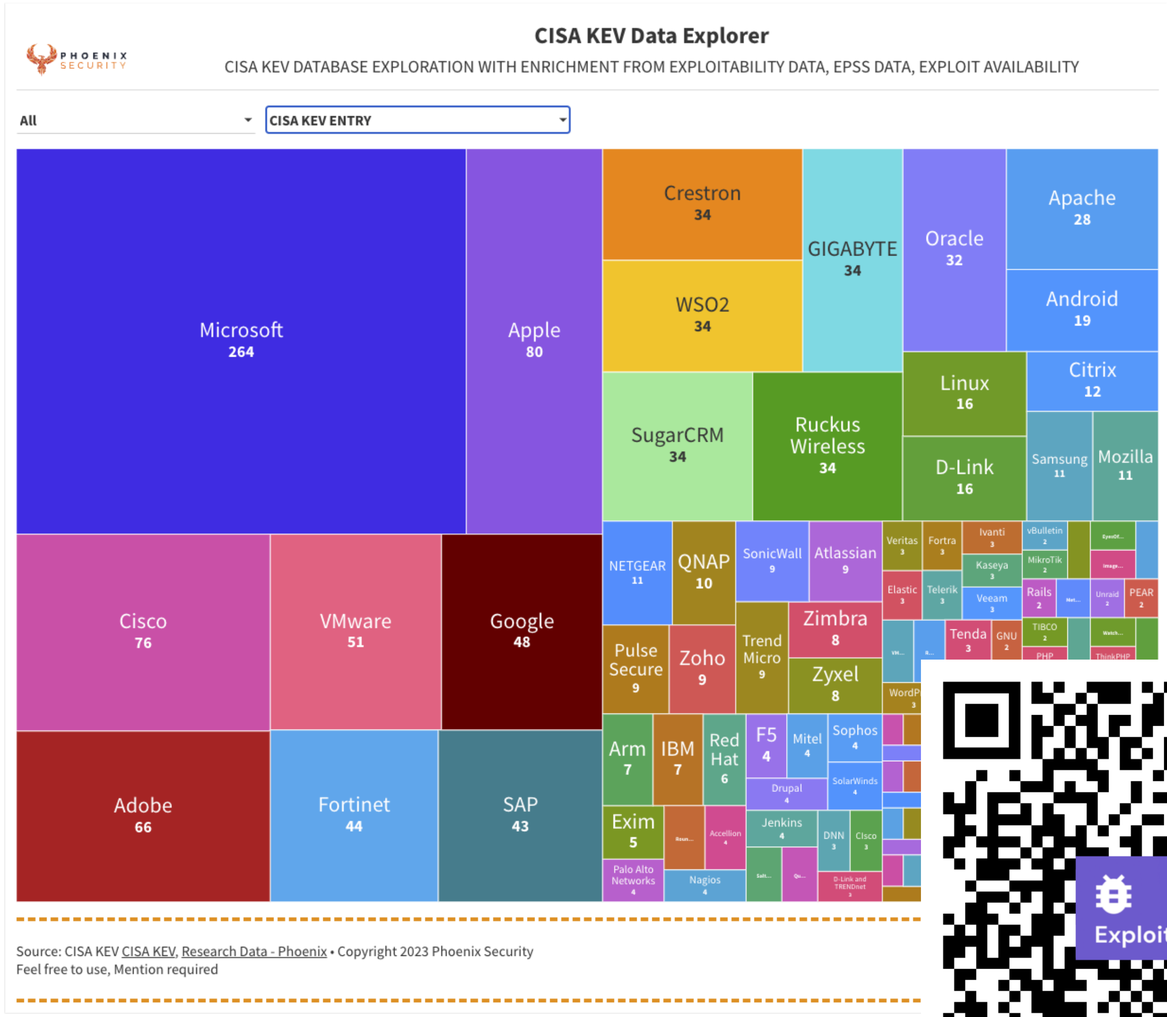
GitHub Active Exploits

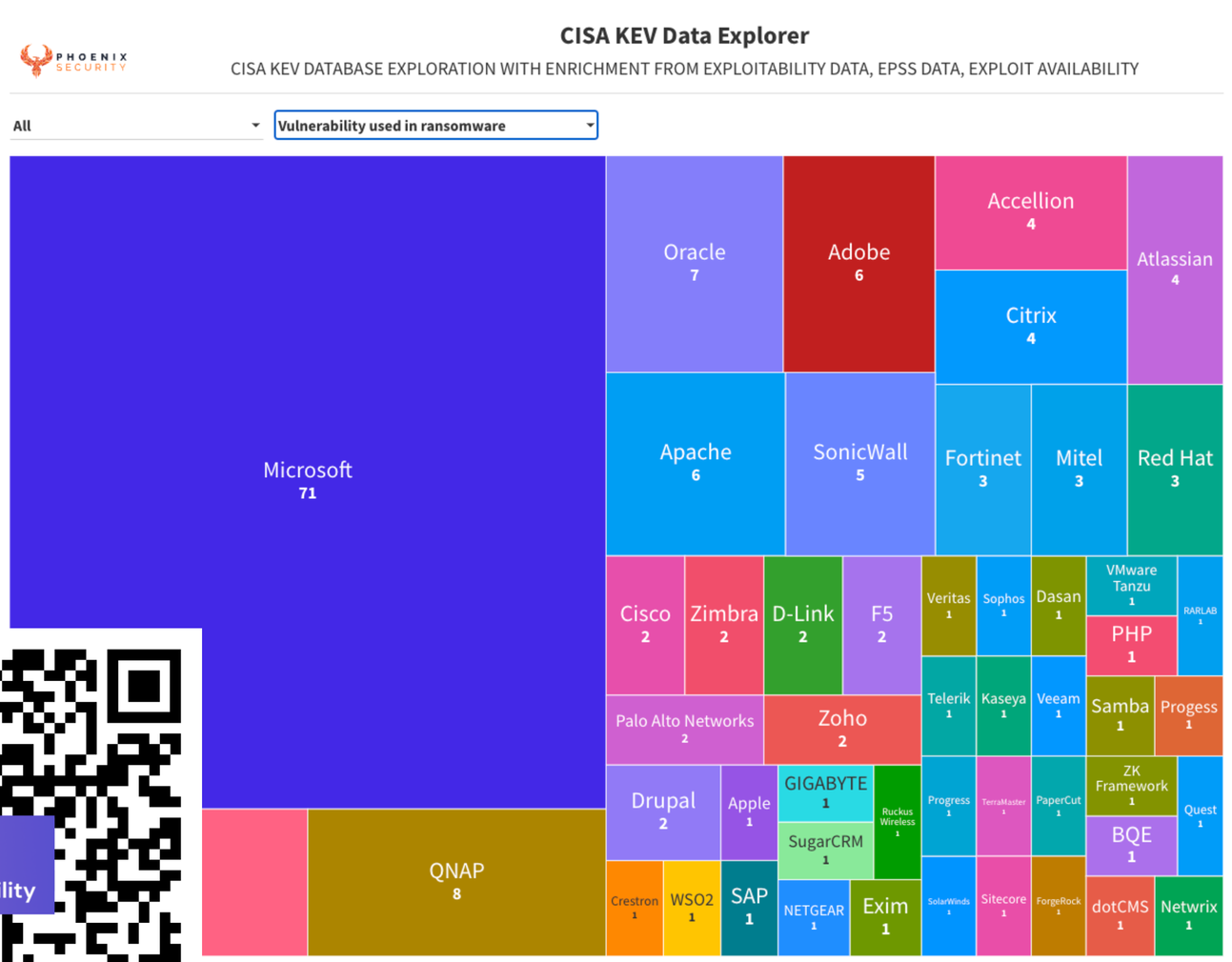


Number of Verified Exploits



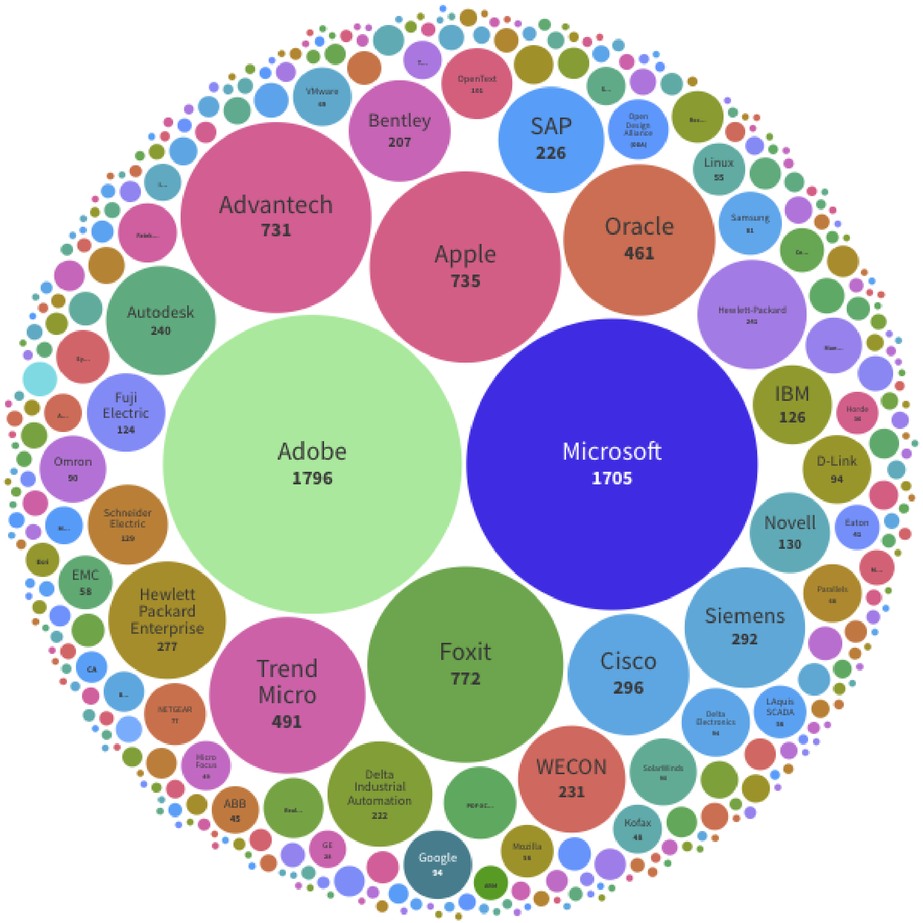
Vulnerabilities used in ransomware



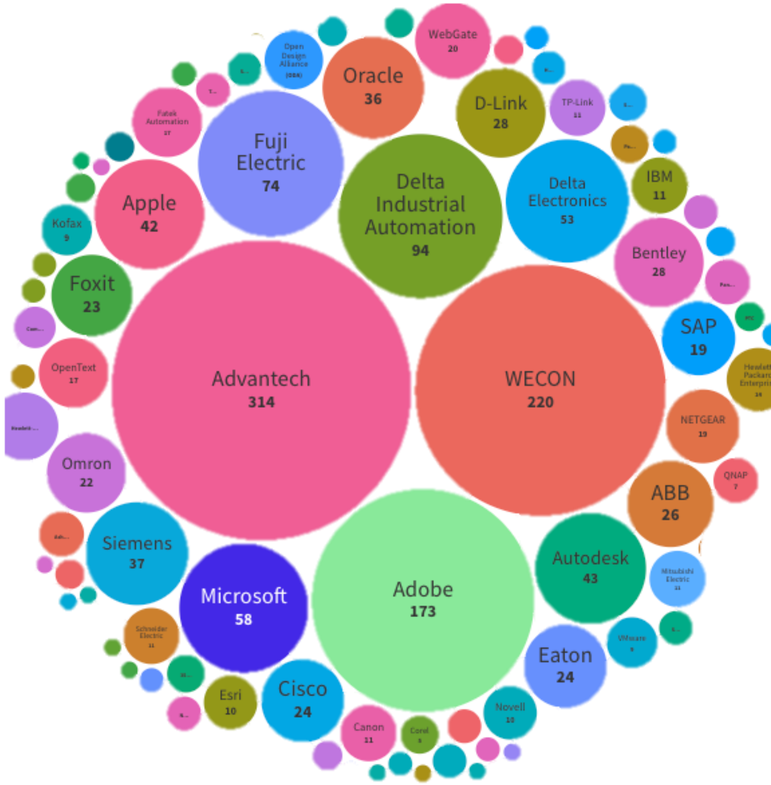


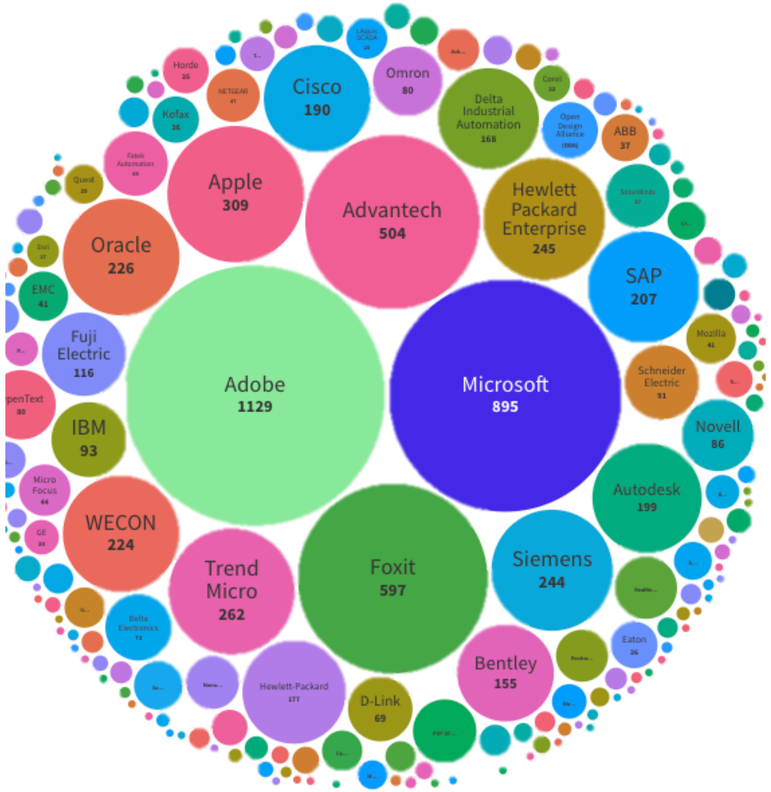
VENDOR WITH MOST ZERO DAY

Exploitability



Buffer Overflow

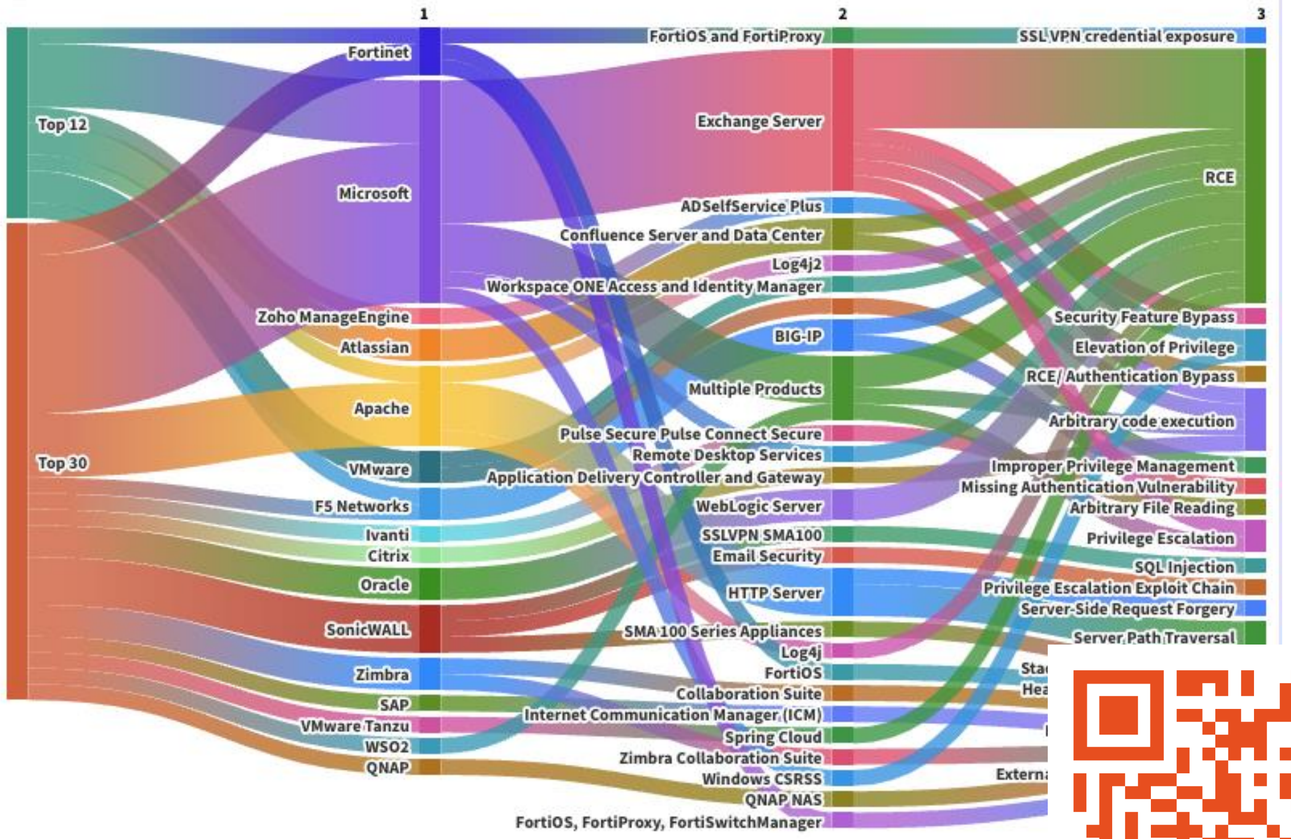




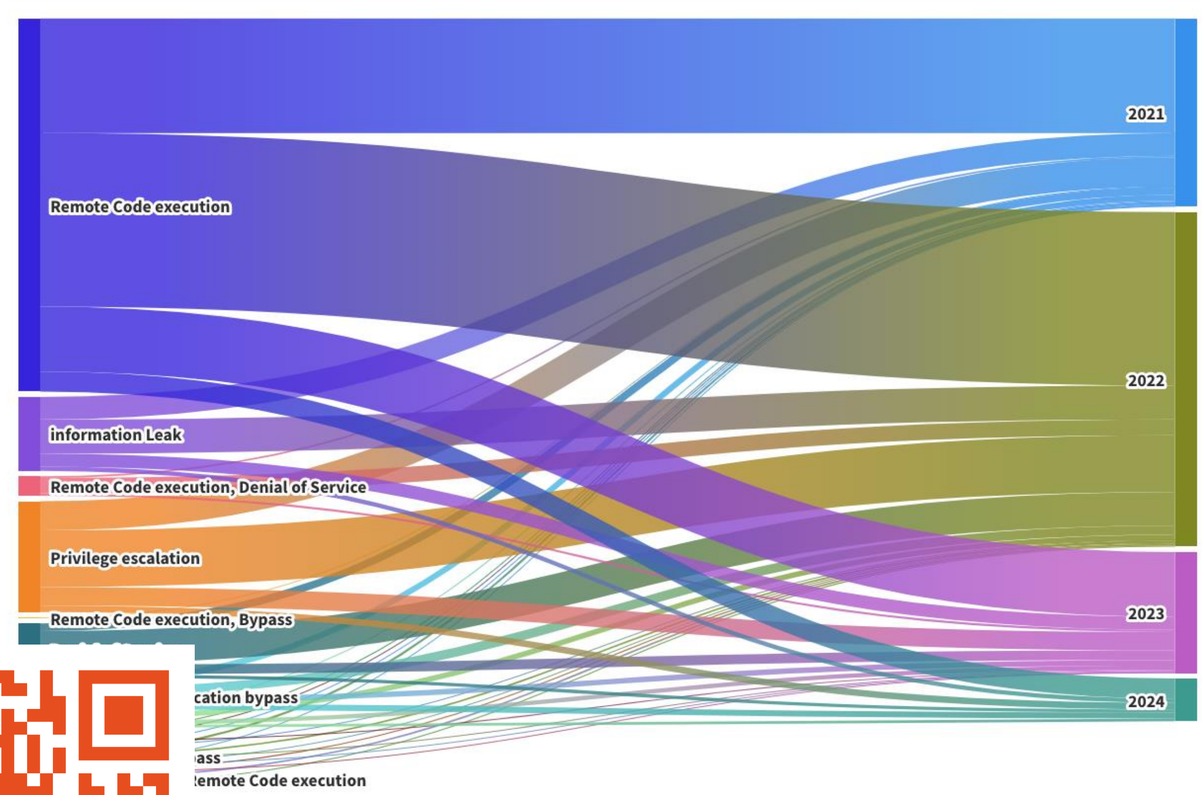
RCE

PHOENIX CTI - MOST USED ATTACK METHODS

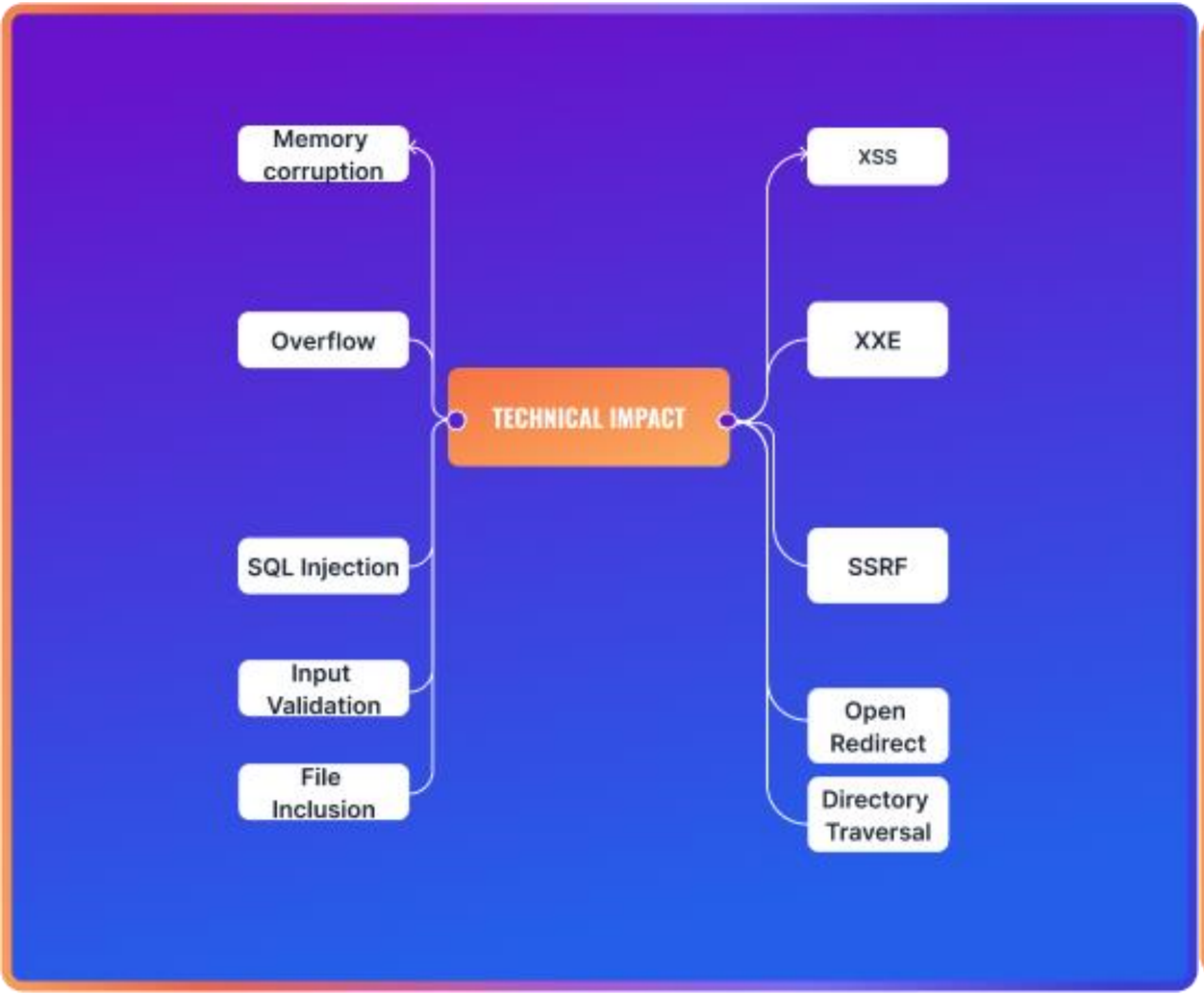
TOP EXPLOITS METHODS



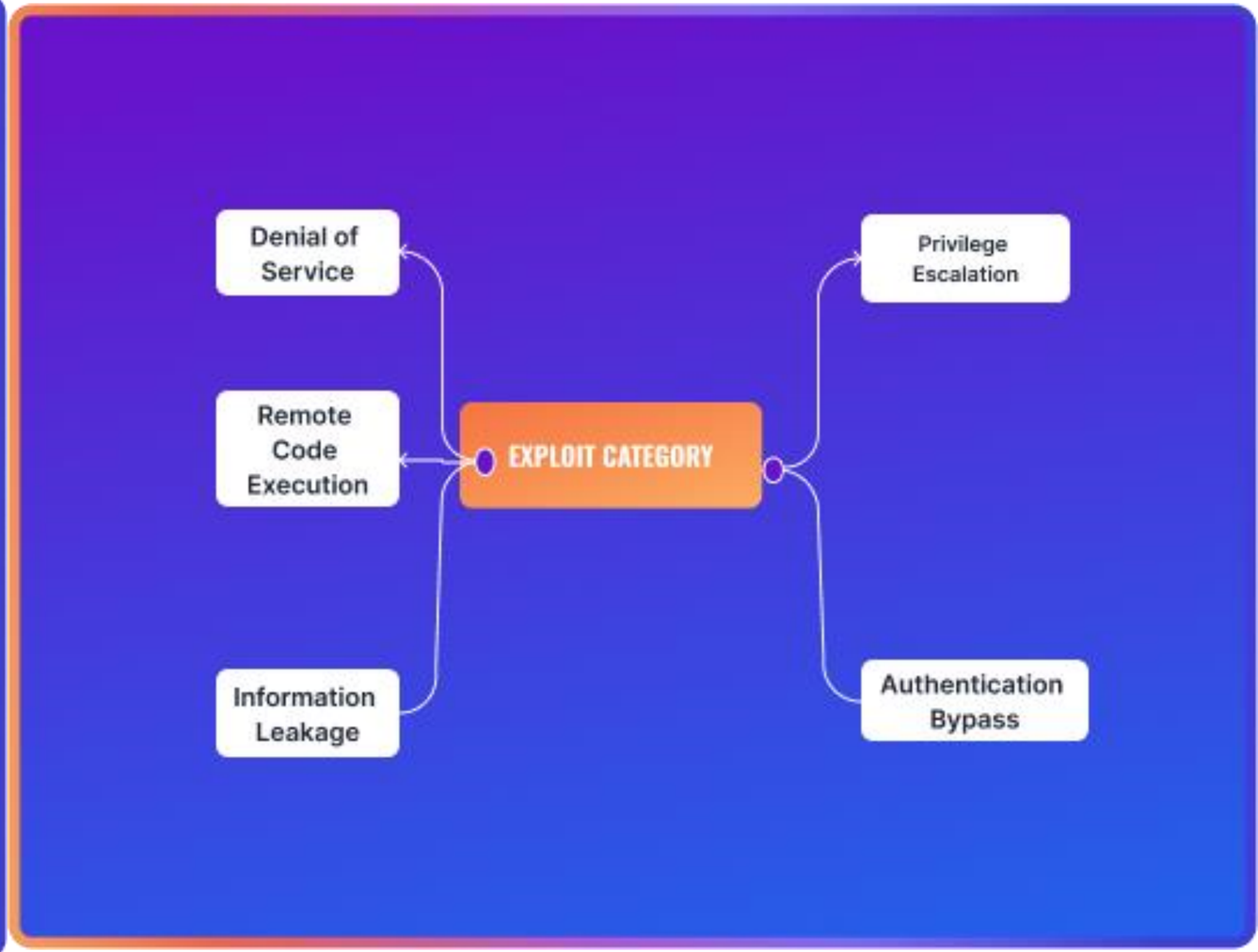
CISA KEV



Anatomy of vulnerability



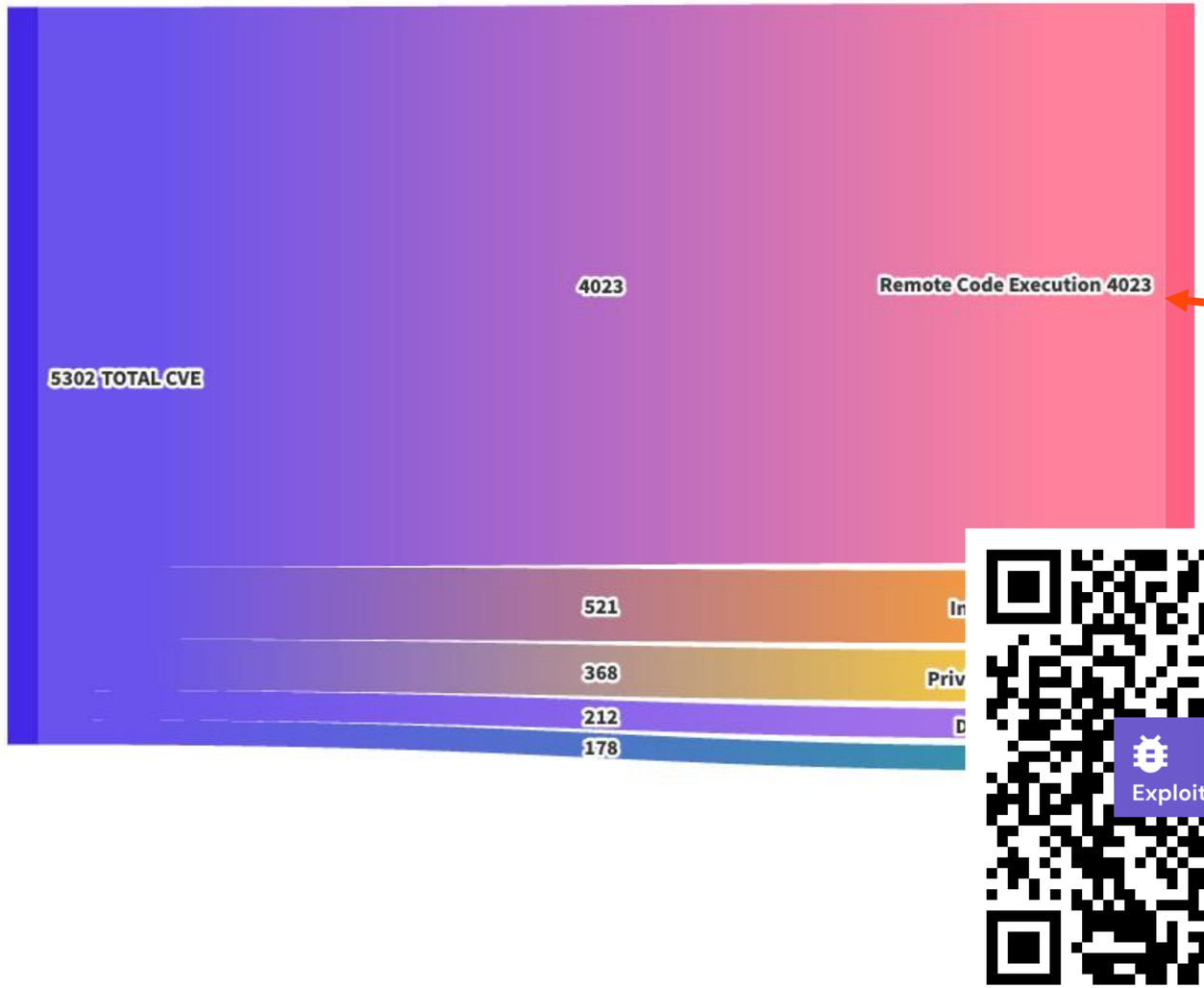
IMPACT OF VULNERABILITIES



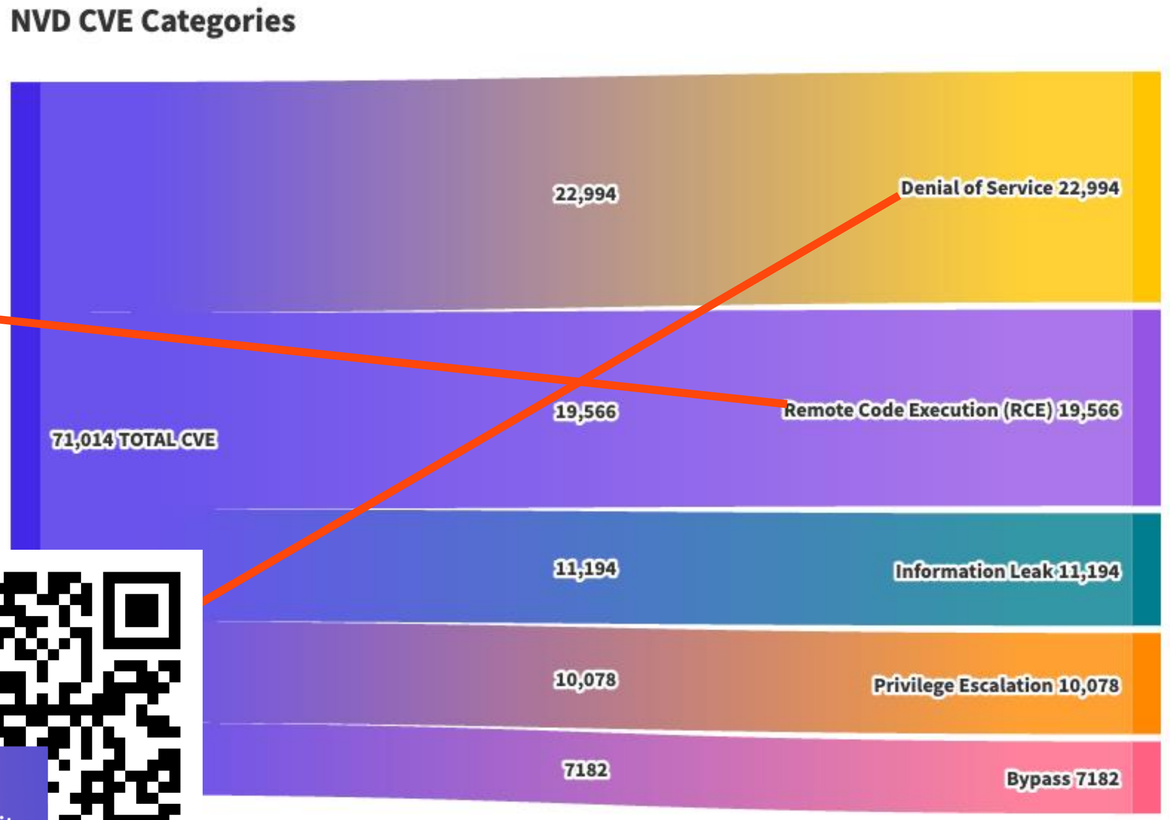
CATEGORY OF EXPLOITS

PHOENIX CTI – GITHUB POC – MOST USED METHOD

TOP EXPLOITS METHODS



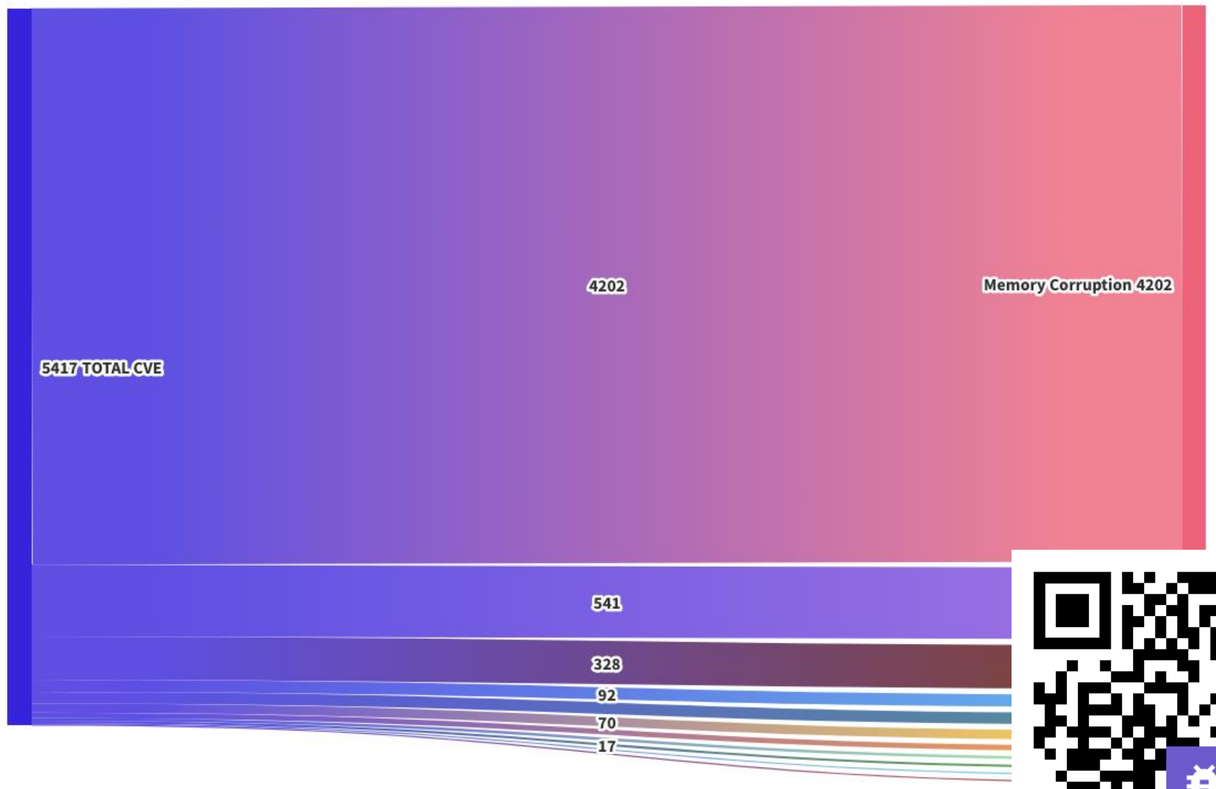
Overall NVD



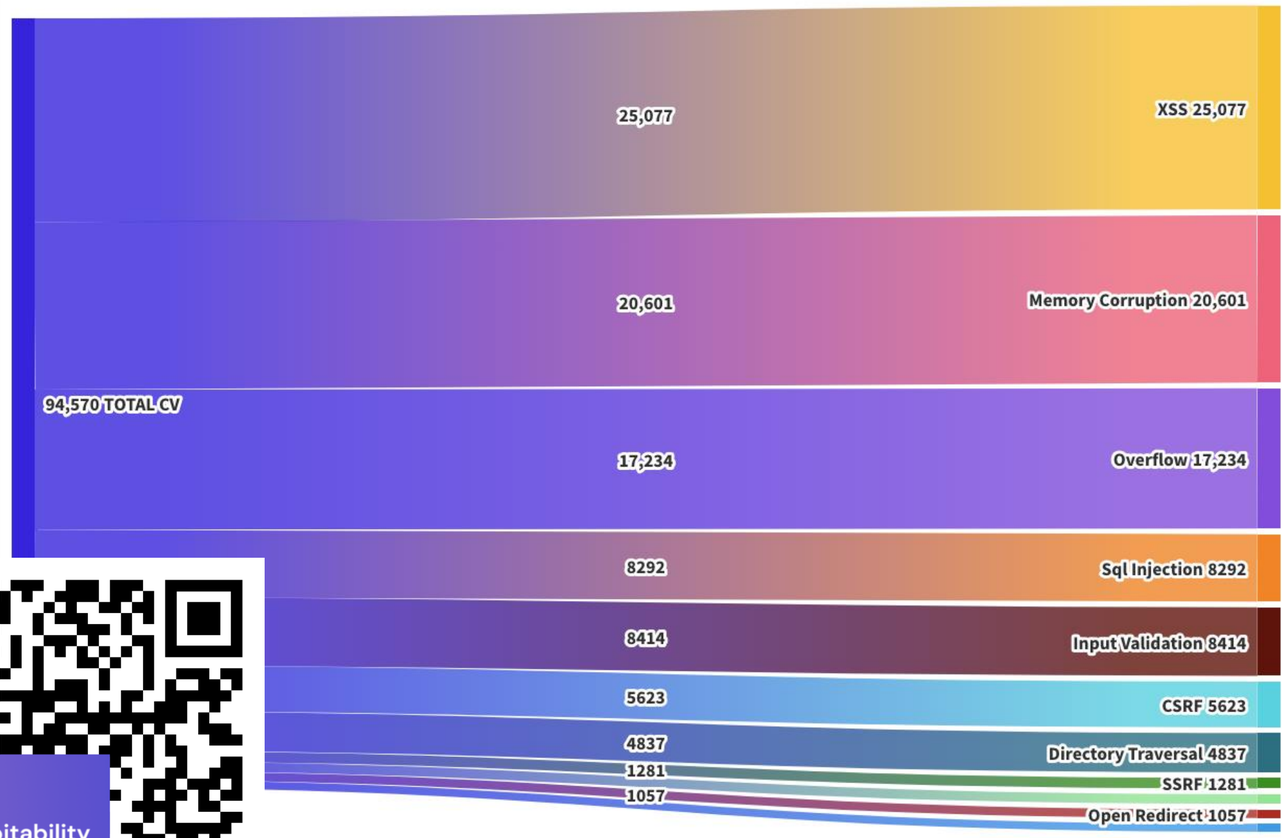
Exploitability

PHOENIX CTI – GITHUB POC – PREVALENT TECHNICAL IMPACT

TOP EXPLOITS IMPACT



Overall NVD

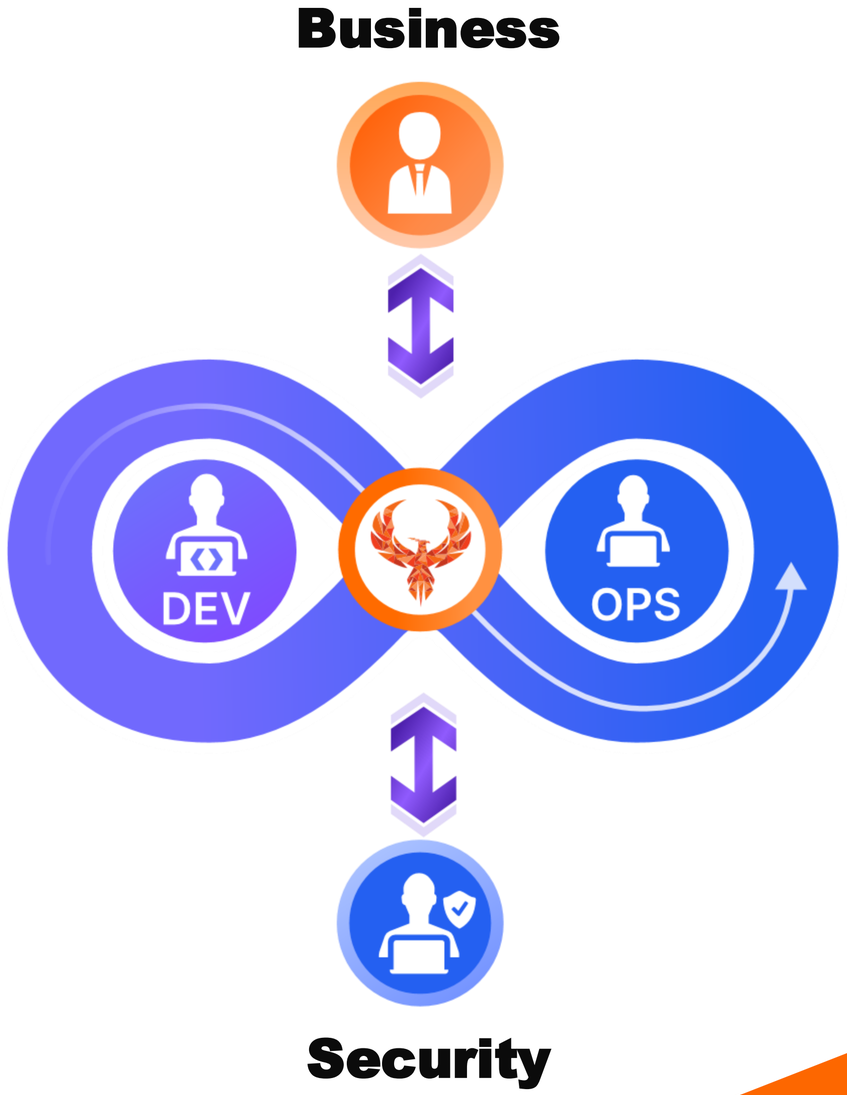


Exploitability

Part 3 - Scaling without an army Data Driven Approach

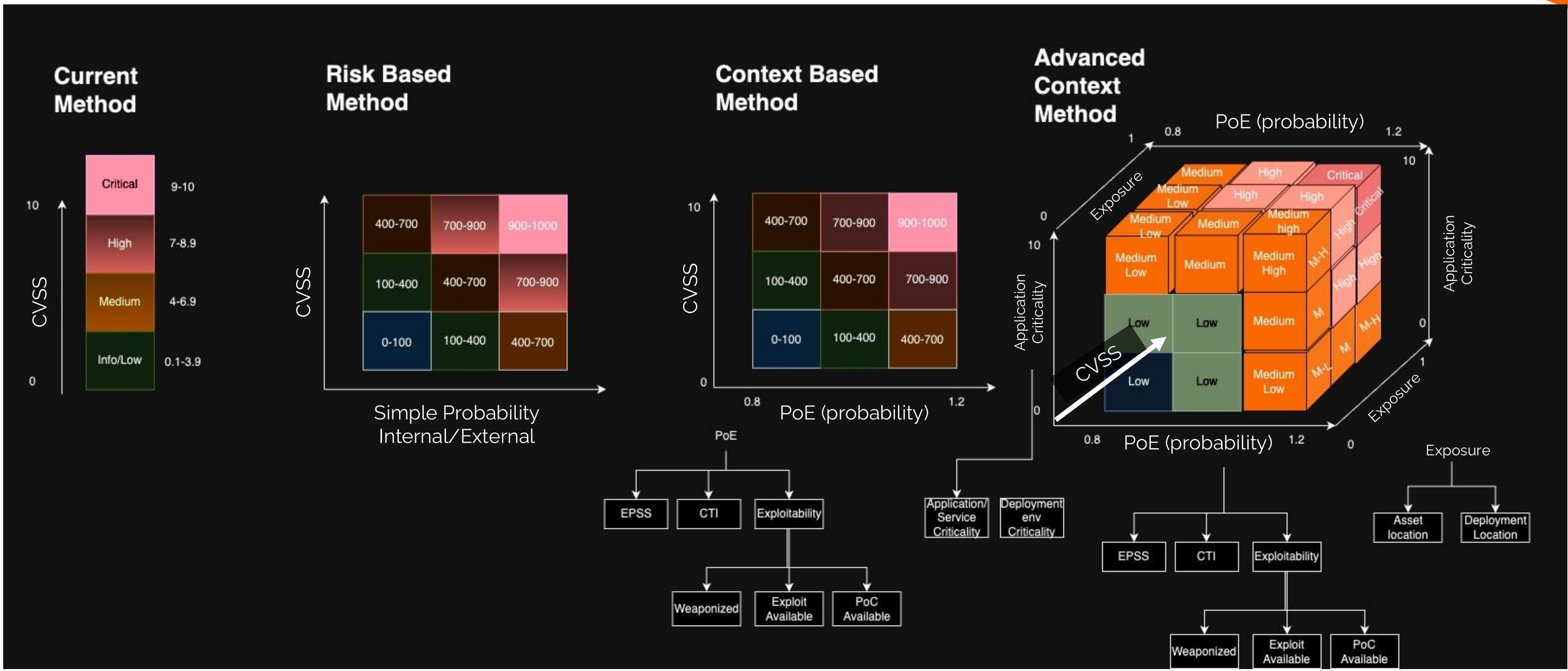
Phoenix Security translates Business Risk objectives into precise actions for engineers

Identifying with Contextual AI the best fix to resolution

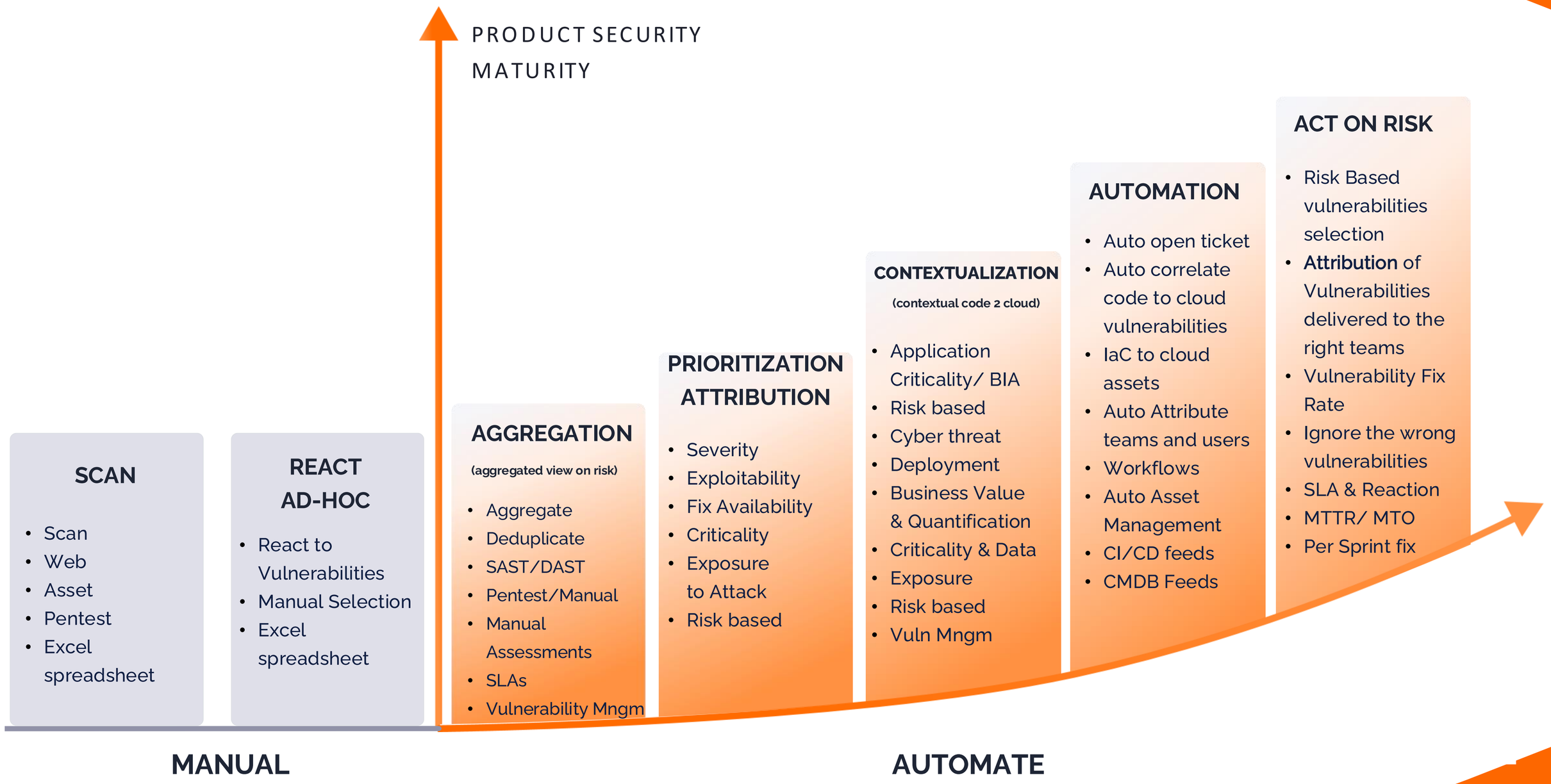


RISK COMMON LANGUAGE

PHOENIX BRINGS OUT THE 4TH DIMENSION OF RISK



WHERE ARE YOU IN YOUR SOFTWARE SECURITY MATURITY JOURNEY?



Conclusions

So we solved security right?

There is a light at the end of the tunnel

- Shift approach, Who does what where
- Application Security + Environment > products and owners
- Top down approach on risk- focus on real risk
- Talk the right language to the right teams
- Focus on patterns and fixes instead of raising problems

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

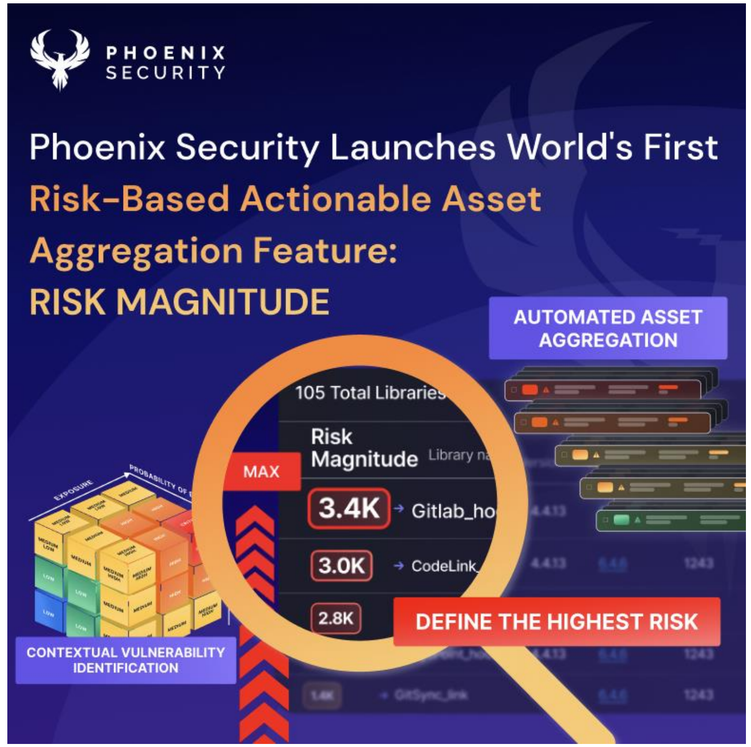
ACT ON SBOM VULN

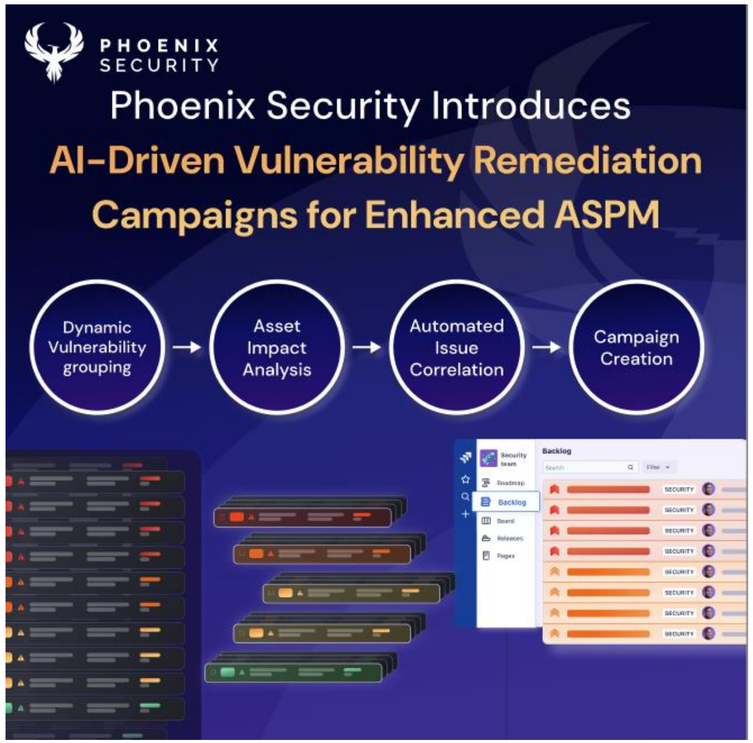
Phoenix Security Unify ASPM & CSPM for a contextual approach

ISC2 CHAPTER LONDON

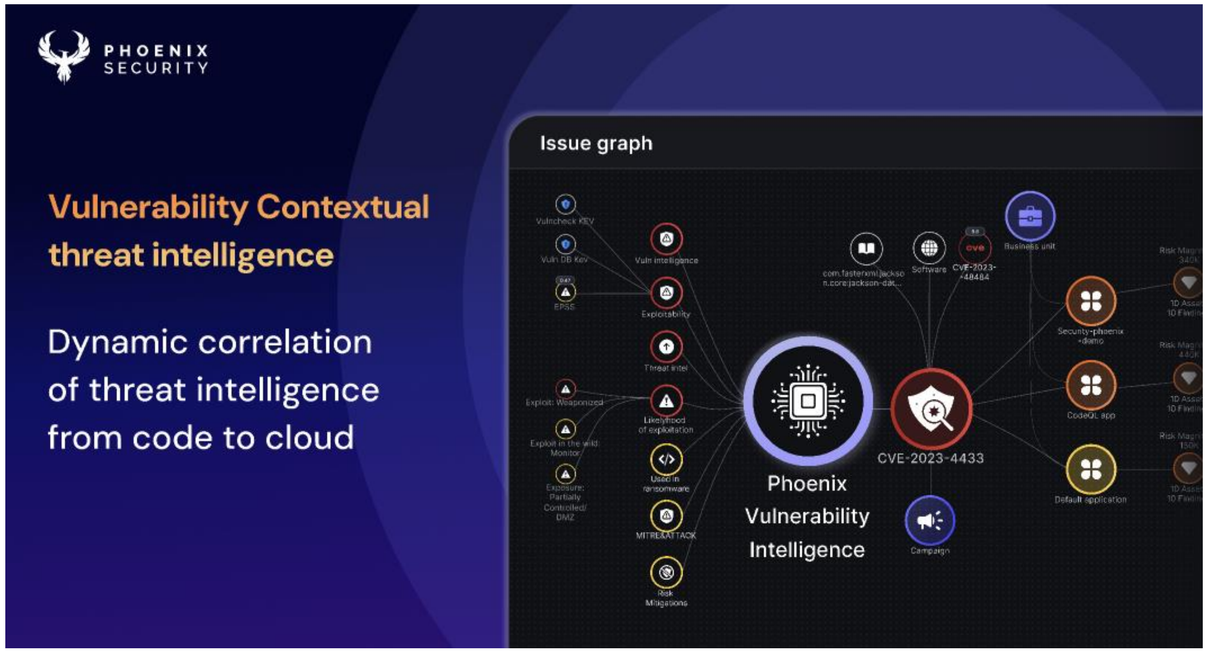
IDENTIFY PROBLEMS	ORGANIZE, PRIORITIZE, CONTEXTUALIZE	ACTIONS ON RISK

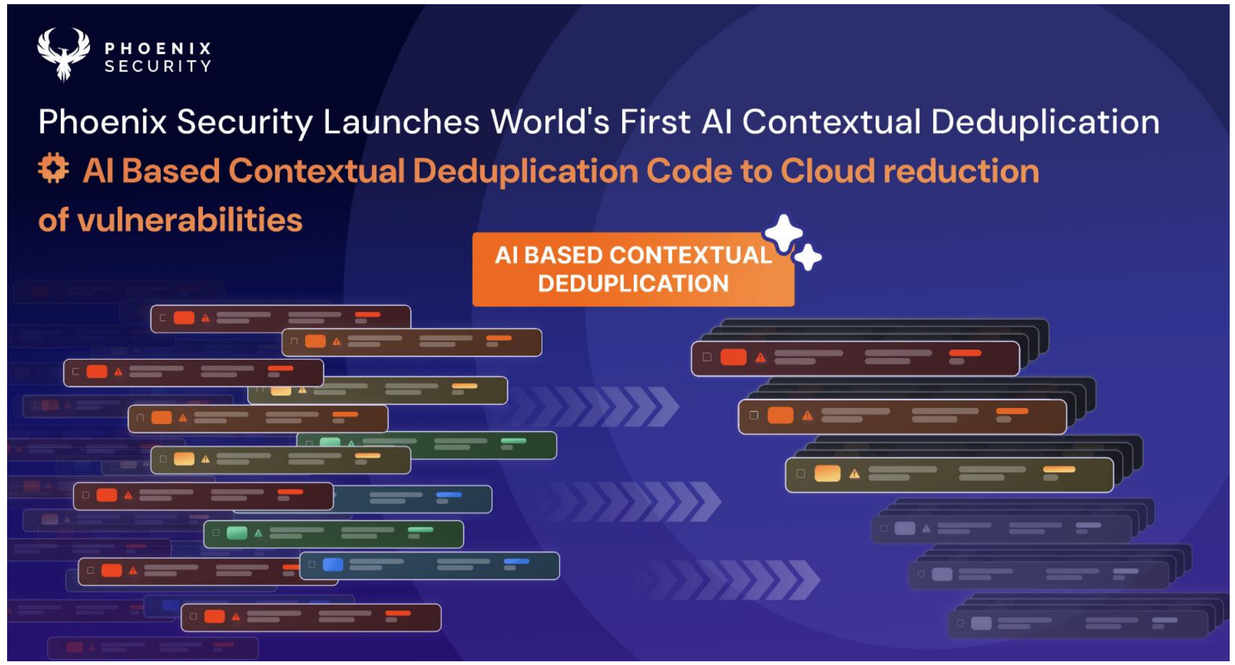
New Features





Upcoming New Features



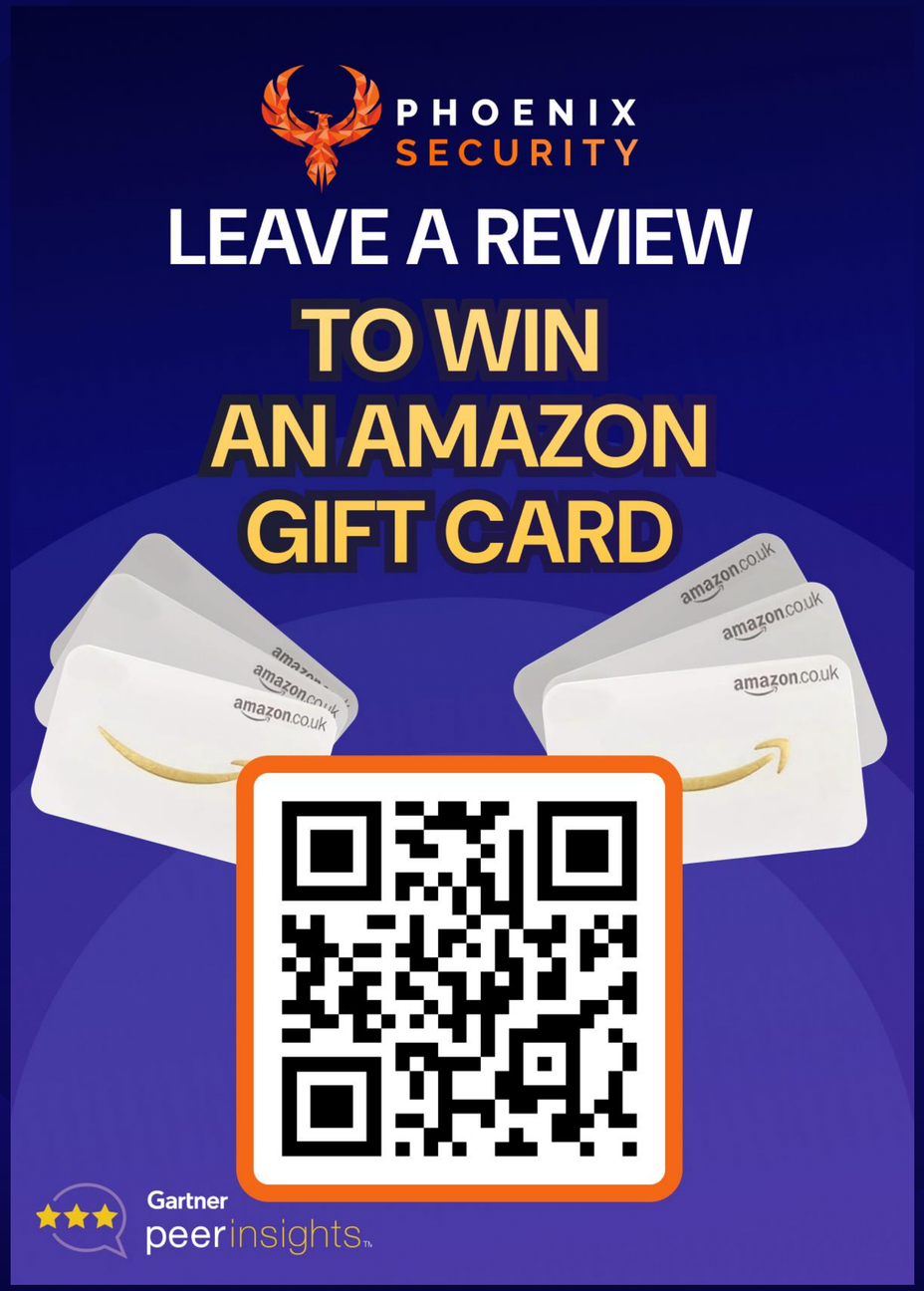


Partnership

Threat Intelligence

Cloud Integrations

Penny for your time (and thoughts)



Get a demo today and provide your feedback

Win an amazon Gift Card

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

PHOENIX SECURITY

ACT ON CONTAINER VULN

ACT ON ENDPOINT VULN

ACT ON CLOUD VULN

CONTEXTUALIZE, PRIORITIZE & ACT ON RISK

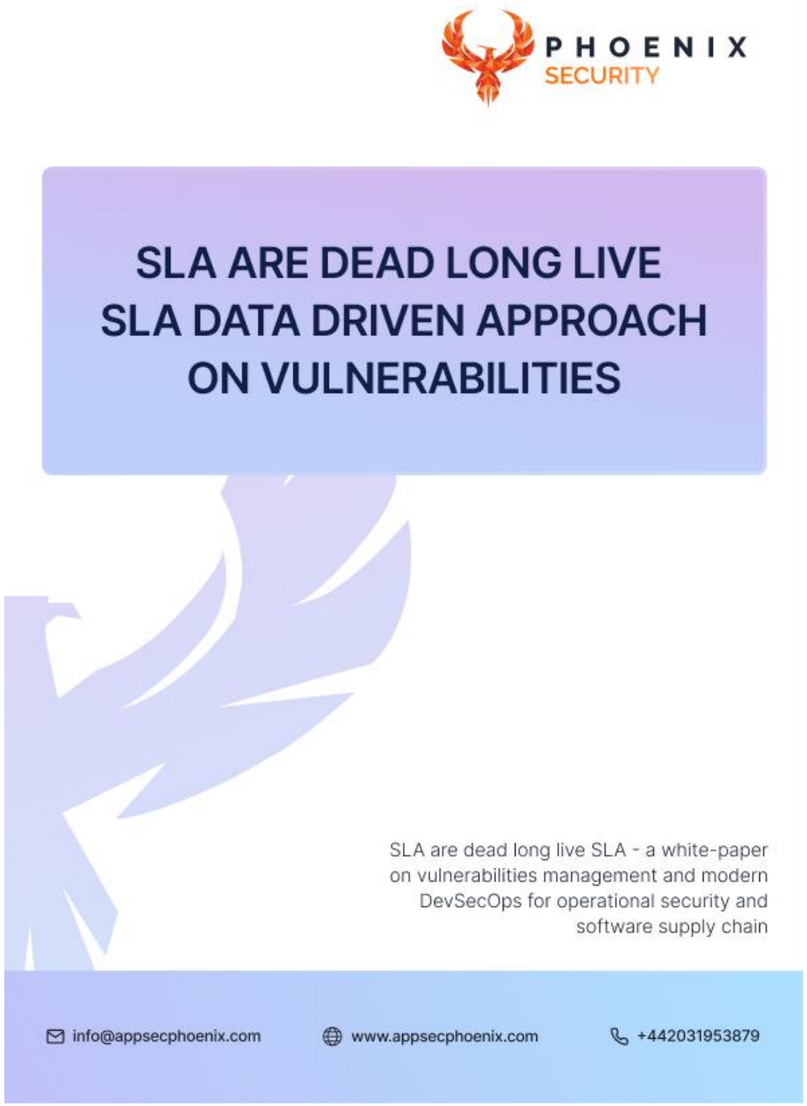
ACT ON APPSEC VULN

ACT ON INFRA VULN

ACT ON CODE VULN

ACT ON SBOM VULN

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

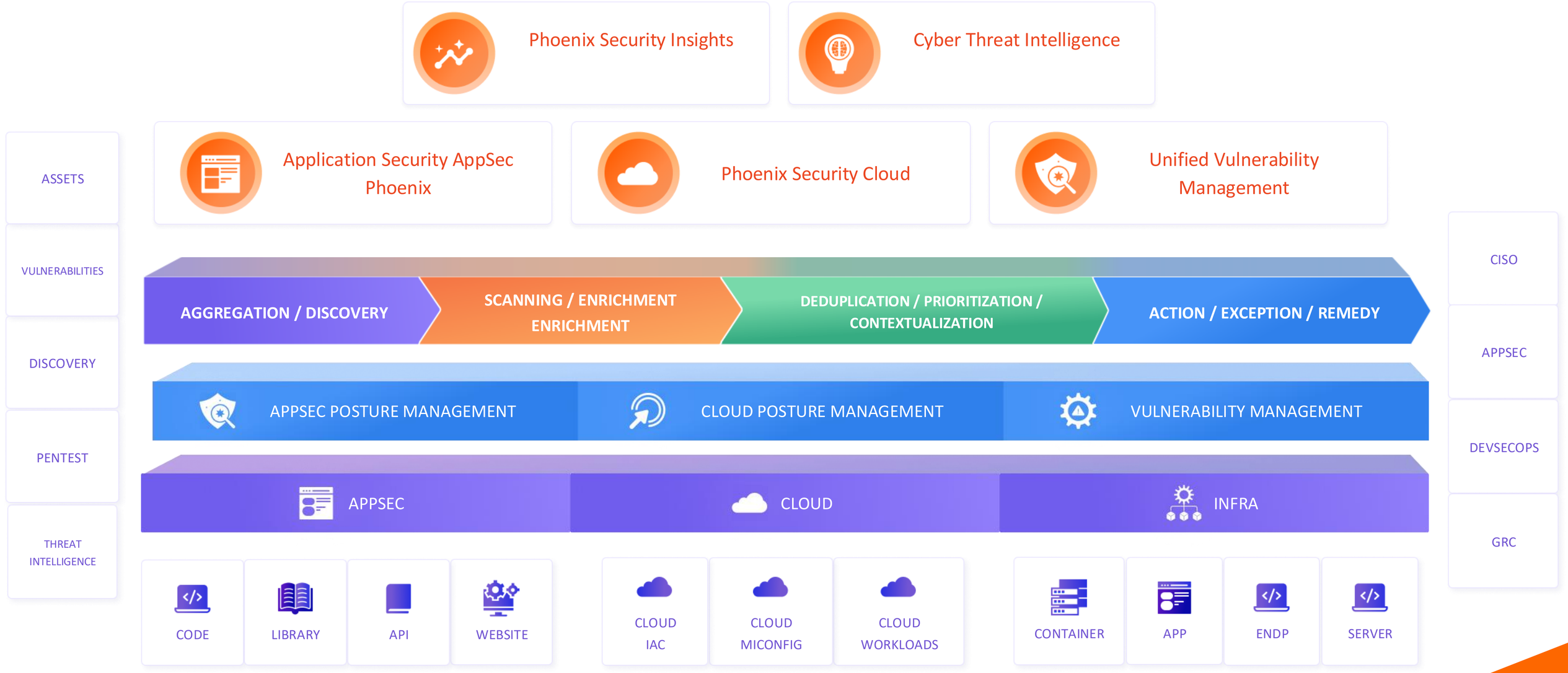
@FrankSEC42

www.cybercloudpodcast.com

Sponsored By

PHOENIX SECURITY

Phoenix Security platform unifies risk across your entire attack surface



CONTEXTUALIZE PRIORITIZE | ACT ON RISK THAT MATTERS MOST

POSTURE MANAGEMENT ACROSS X SURFACES E(X)SPM

ISC2 CHAPTER LONDON

eXtended Surface Posture Management (XSPM)

- ASPM
- RBVM
- Cyber Asset Management
- Team performance tracking/ Attribution/ Traceability
- Correlation of asset across domains (library from SCA and container)
- Deployment traceability with canaries
- Cloud Based Vulnerability Management

EXTENDED SURFACE POSTURE MANAGEMENT XSPM

Secure Runtime, Application

in one view empowering business to make risk based decision actionable from engineers / developers

ASPM Application Posture management

Prioritize fixable cloud native application/ scanning and recheability

- Aggregation of multiple assets classes
- Deduplicate/ Correlate/Prioritize assets and vulnerabilities
- Attribution of team to code
- Traceability of application to cloud
- Prioritization based on deployment

Identify what's fixable based on the deployment of deployment of the application

EASM External Attack Surface Management

Scan your external attack surface and correlate with internal surface

- Correlation and contextualisation of internal and external
- Threat intelligence and prioritization of the vulnerabilities
- Correlation with application/deployemnt
- Correlation with application

Identify what's important to work on from outside in

Risk Based Vulnerability Management

Manage internal vulnerability with risk based prioritization

- Prioritize vulnerability using threat intelligence
- Aggregate asset classes and extract insight across multiple sources
- Dedupliacte, Correlate, cross domains
- Attribution and Application treceability

Trace application on prem-cloud and correlate threat inel

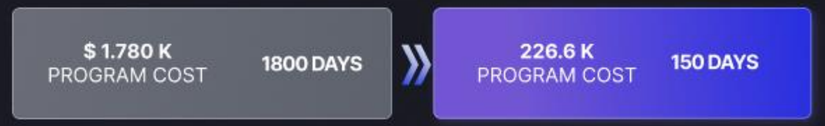
CSPM Cloud Security Posture Management

Prioritize internal vulnerability in the cloud and create internal/external attack surface

- Traceability of applicaiton to cloud deployment
- Conceptual segmentation of production
- Correlate Container and cloud pre-post flight
- Transfer insight cross domain (e.g. recheability of an application

Trace application on cloud-cloud and correlate threat inel

Removing Manual work to automate, scale effectively security teams



DESCRIPTION	Without AppSec Phoenix COST	Without AppSec Phoenix TIME	APPSEC PHOENIX (7X CHEAPER, 12X FASTER) COST	APPSEC PHOENIX (7X CHEAPER, 12X FASTER) TIME
TOTAL	**$2,983.00**	**24h**	**$376.00**	**2h**
Export of report/ Vulnerabilities	$56.00	30 min	$0.00	0 min
Notification to Security professional	$3800	20 min	$0.00	0 min
Analysis of reports by DevSecOps	$600.00	320 min	$59.38	15 min
Perform Vulnerability Assessment	$375.00	200 min	$59.38	15 min
Contact the business owner and assess the importance of the application	$375.00	200 min	$0.00	0 min
Research exploitability from different databases & Calculate Vulnerability Matrix	$375.00	200 min	$118.75	30 min
Select subset vulnerabilities to execute across platforms	$338.00	180min	$0.00	0 min
DevSecOps Follow-up with developers on schedule and resolution of vulnerabilities. Assume 1 DevSecOps and 2 devs for 2 meetings	$713.00	180 min	$119.00	30 min
Monitoring resolution of vulnerabilities & follow up on targets with DevOps Teams	$113.00	60 min	$19.00	10 min

*DevSecOps average daily rate 500$,
Dev average daily rate 300$