VULNERABILITY MANAGEMENT & SSDLC Workshop

PHOENIX SECURITY

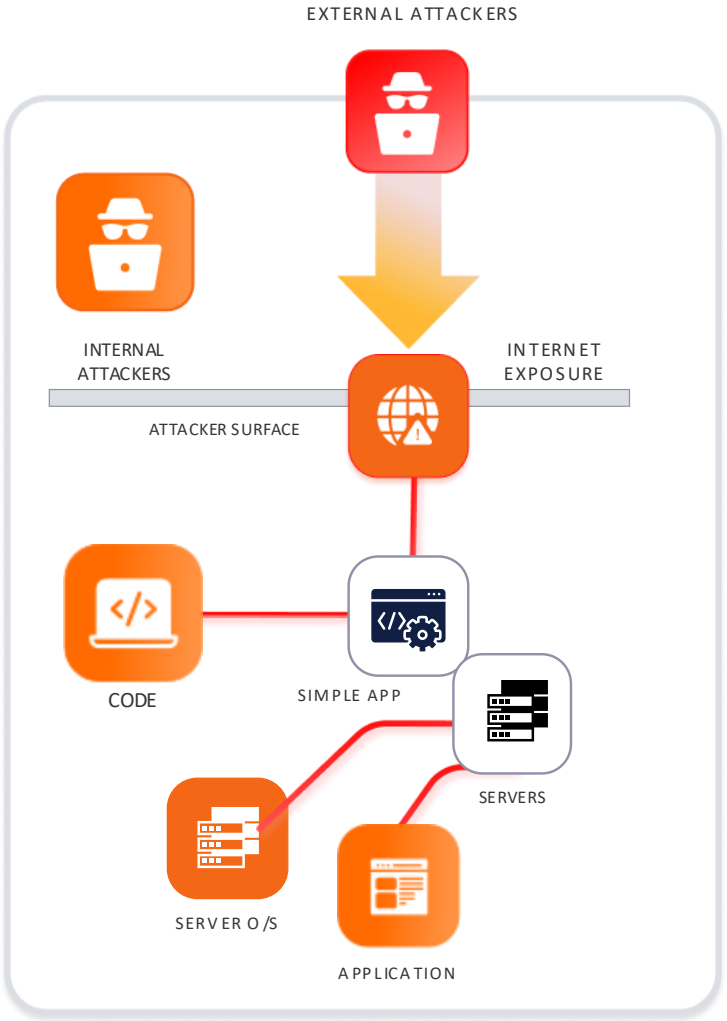
Francesco Cipollone, Co-Founder Phoenix Security, fc@phoenix.security

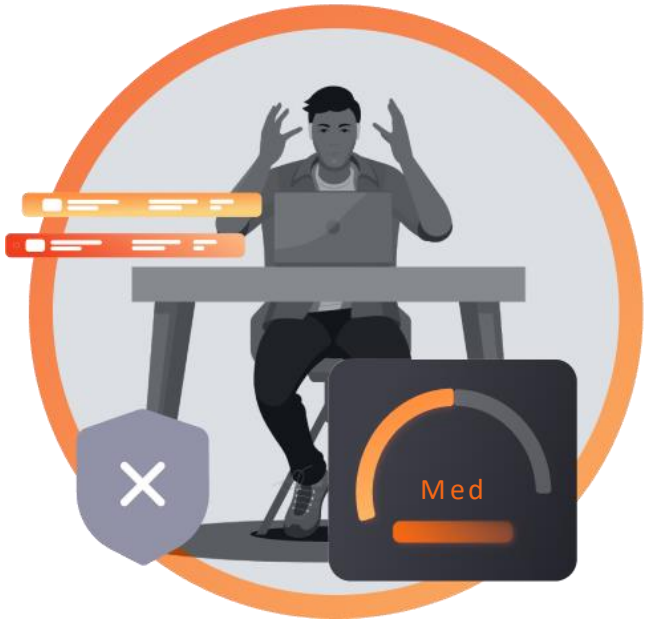
Agenda – OWASP

- Intro
- Where we were and are now?
- Current Challenges
- Vulnerability challenges
- Reachability & reporting lines
- SSDLC security
- Vulnerability Prioritization Methods
- Vulnerability Maturity Model
- VMM – Maturity for Detection and Metrics
- Metrics
- Conclusion - Q&A

Current Challenges

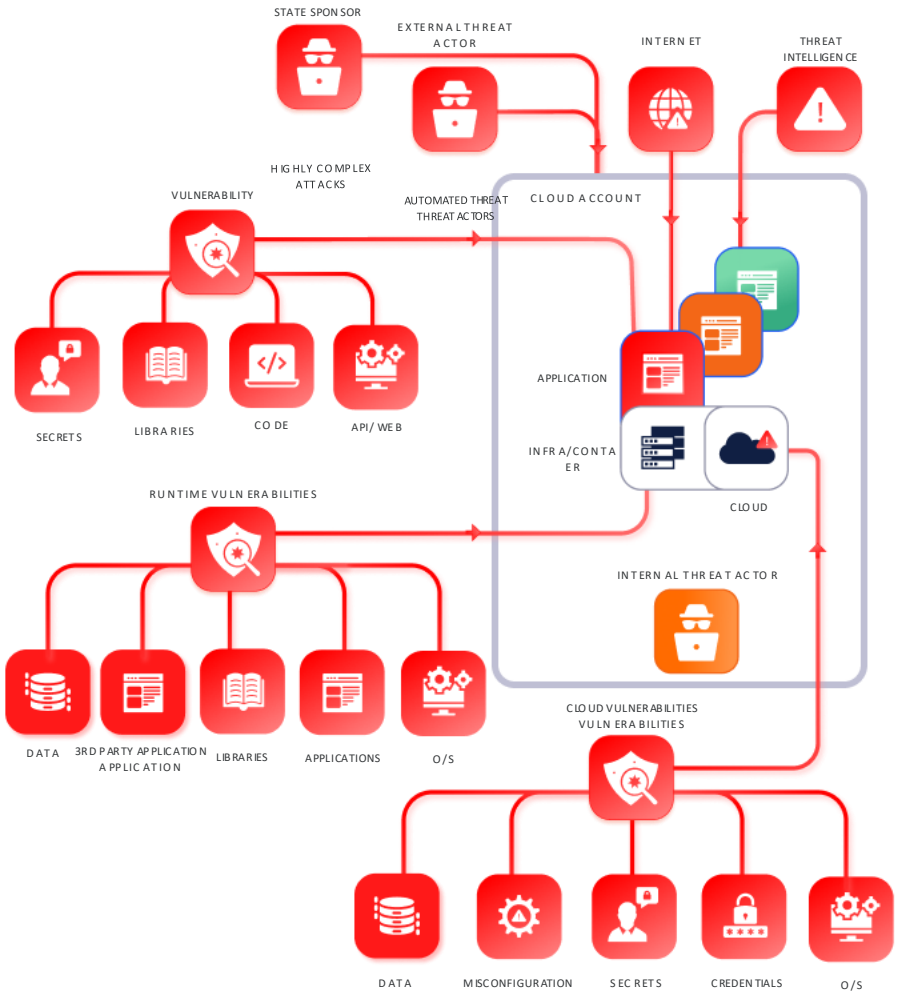
Context: In 2015 we had fewer security tools, digital software supply chain was simpler, and the attack surface was smaller, so finding fixes was trivial

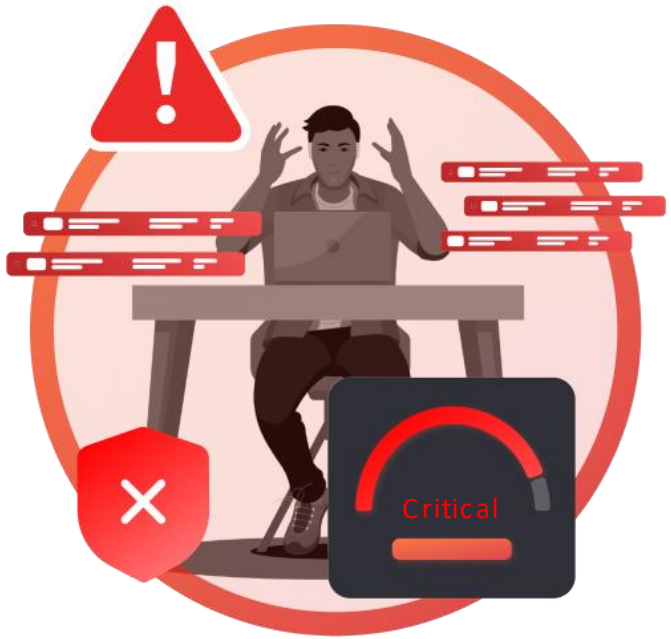




- Total Number of CVEs: 15 K (now 222 K+)
- Few scanners / limited attack surface
- Monolithic software deployed on premises

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**


I feel your pain
OWASP 2024 GLOBAL AppSec
3RD PARTY LIBRARIES
DEVELOPERS
THREAT INTELLIGENCE & CONTEXT
APPLICATIONS
O/S
ENGINEERS
LIBRARIES
O/S
APPLICATIONS
API/ WEB
OEM SOFTWARE
DEVELOPERS
INFRASTRUCTURE VM/LAPTOPS
ENGINEERS
CODE
CODE
CONTAINERS
MISCONFIGURATION
CONTAINERS
APPLICATIONS
CLOUD
DEVELOPERS
CREDENTIALS
CLOUD WORKLOADS
ENGINEERS
LIBRARIES
WEB/API
SECRETS
CLOUD WORKLOADS
Alert FATIGUE
No COMMON LANGUAGE
=
BURNOUT
© Phoenix Security 2024

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

CVE 220,538 **

35% YoY increase

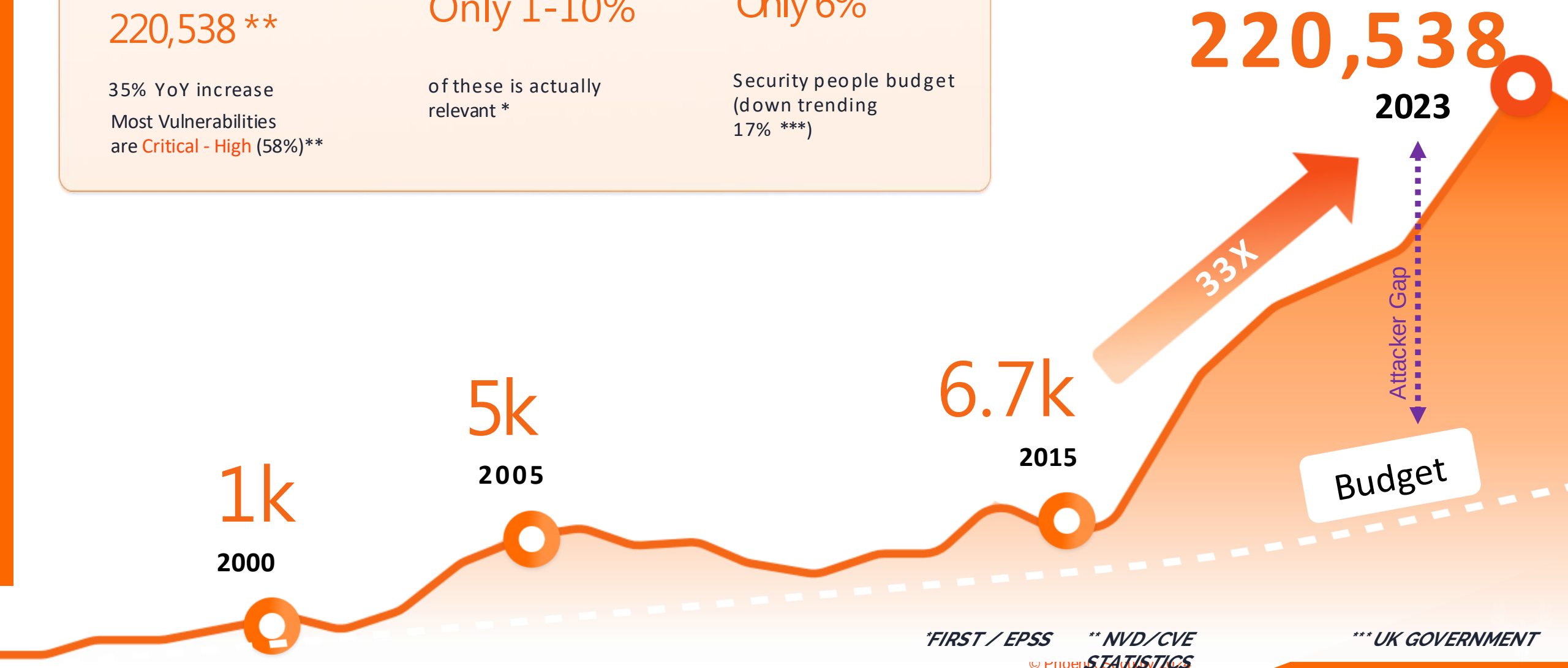
Most Vulnerabilities are Critical - High (58%)**

Only 1-10%

of these is actually relevant *

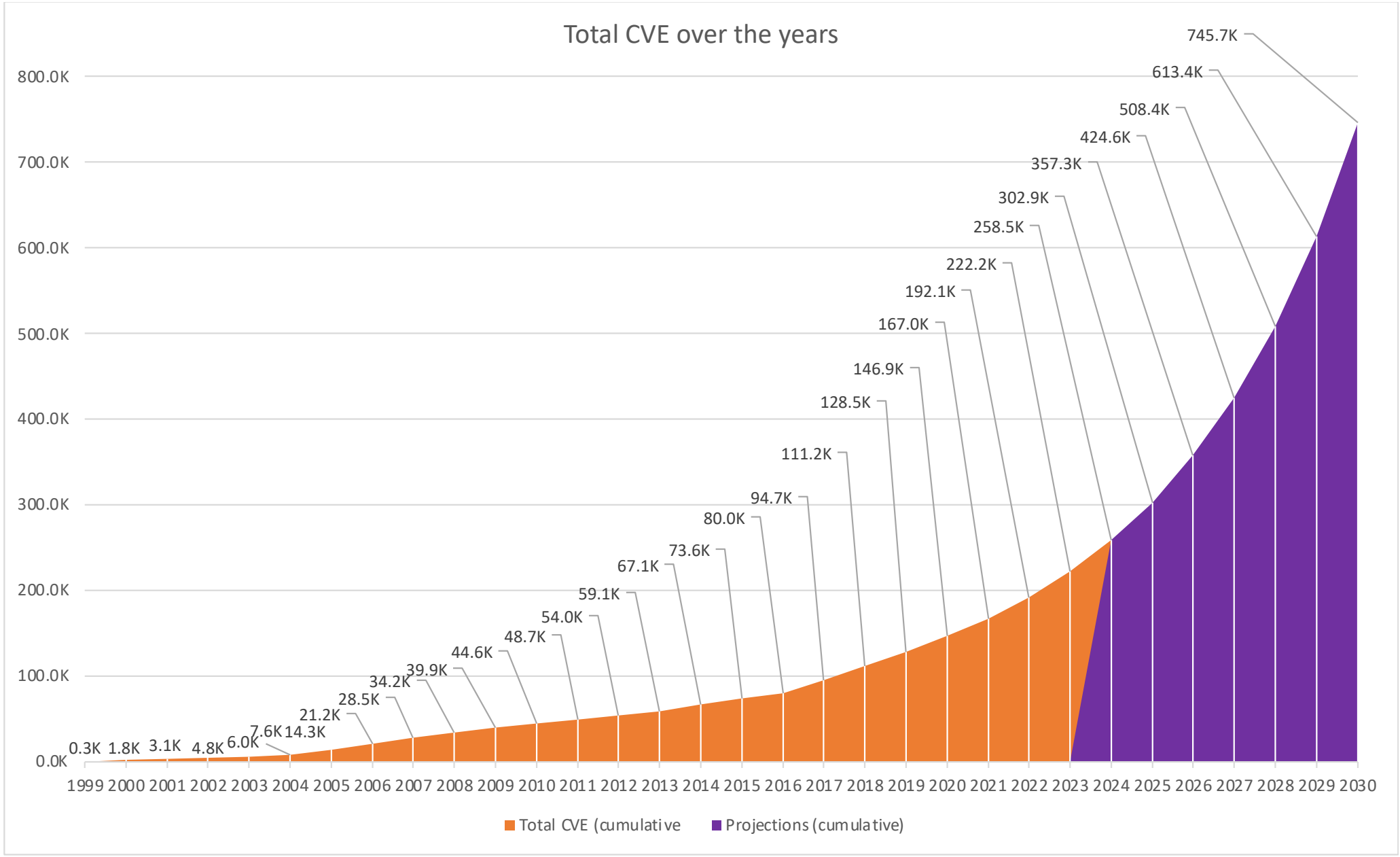
Only 6%

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

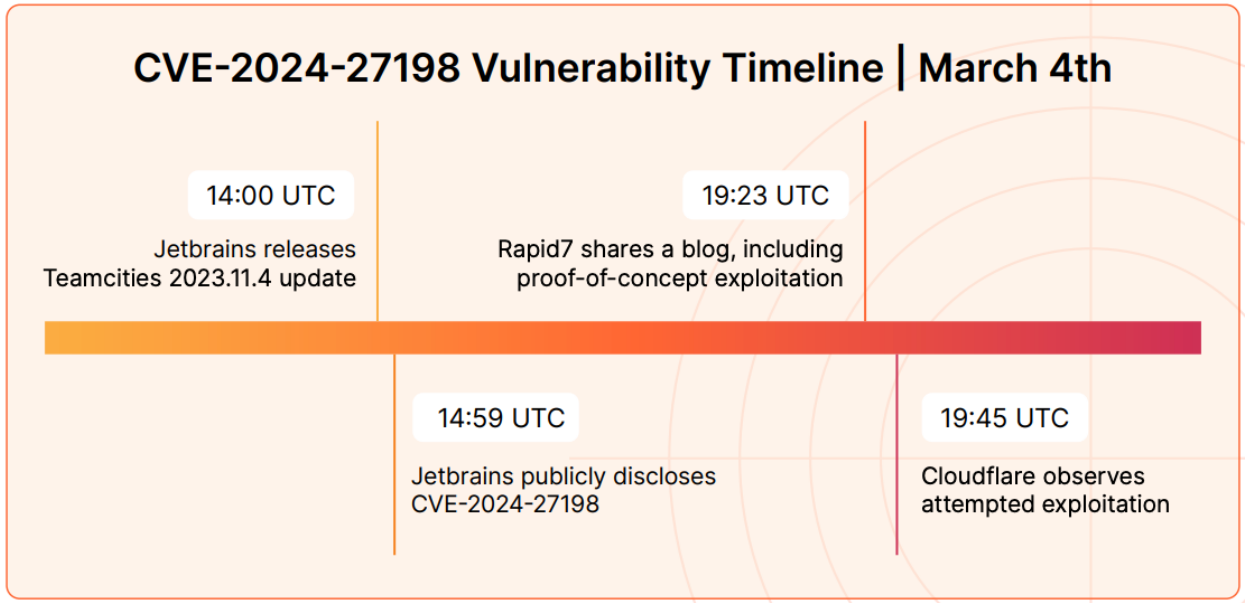
State of Malicious underground LLM to develop malicious code*

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.

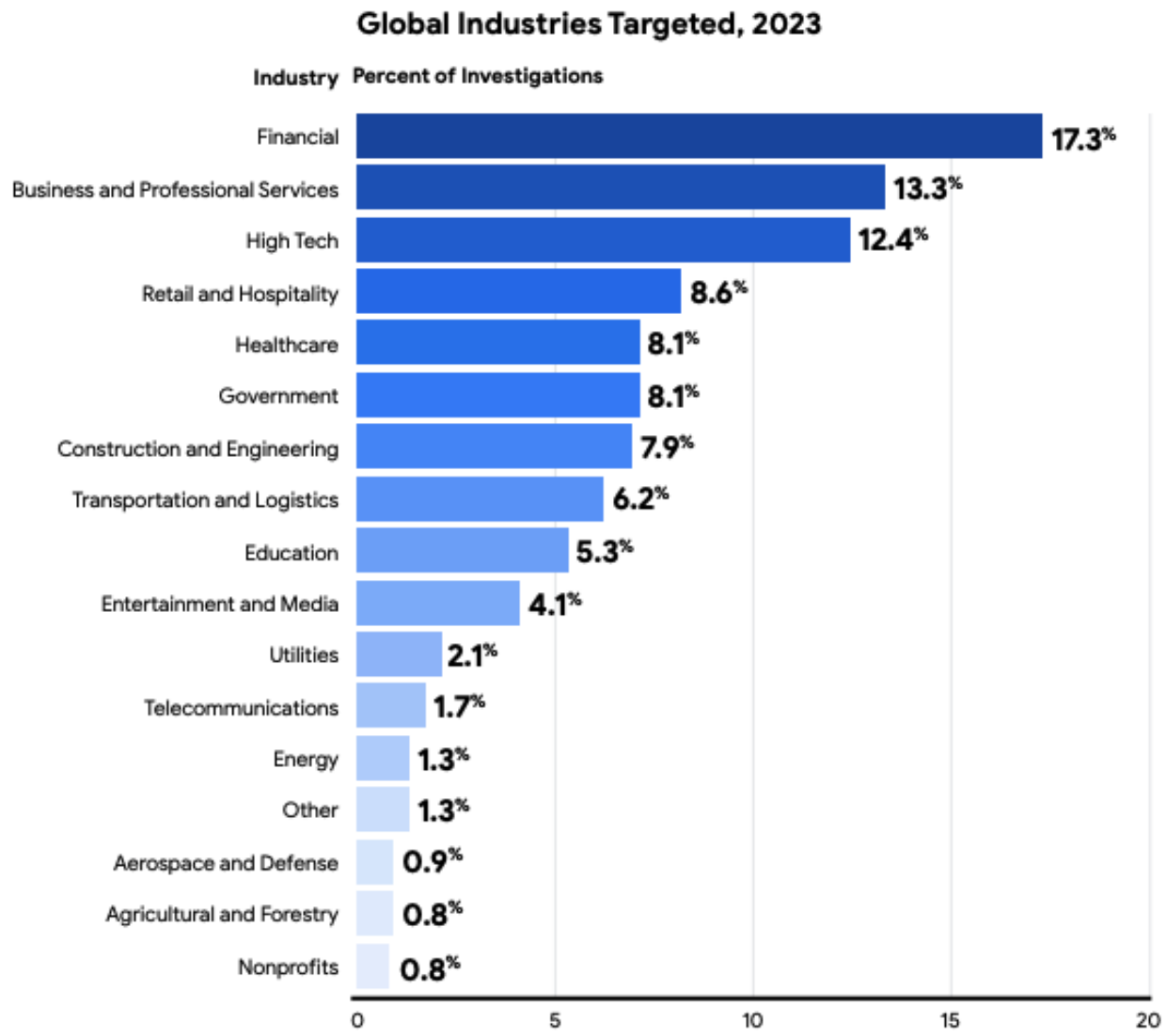
*https://arxiv.org/abs/2401.03315

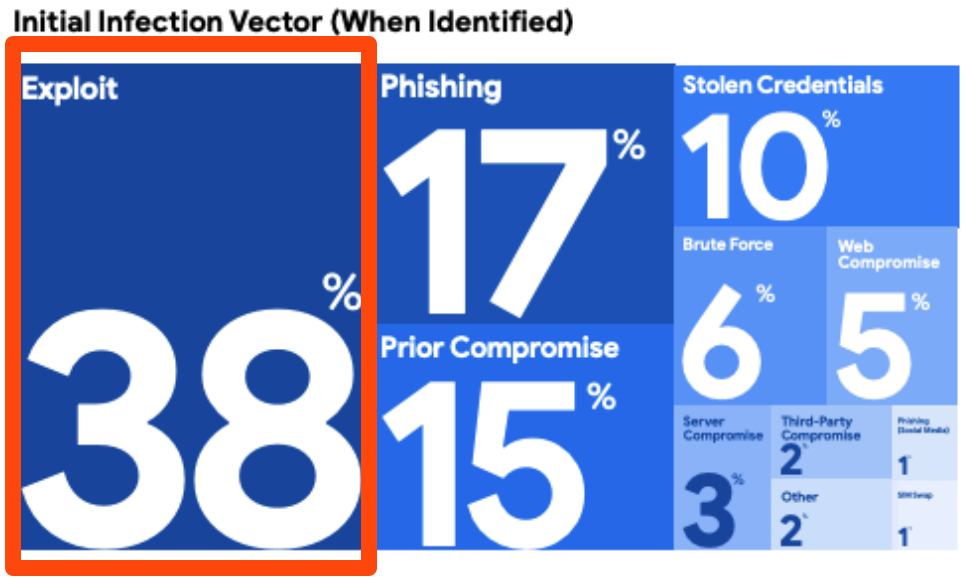


← 3 Minutes** →

**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

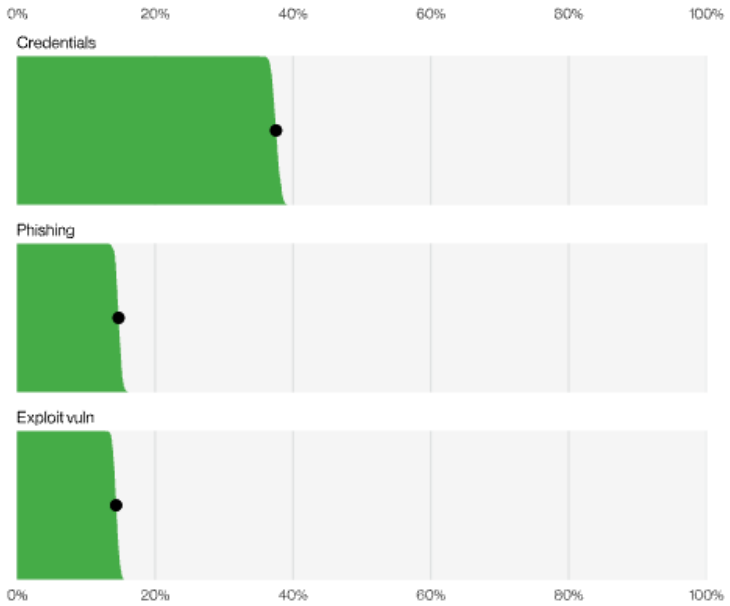
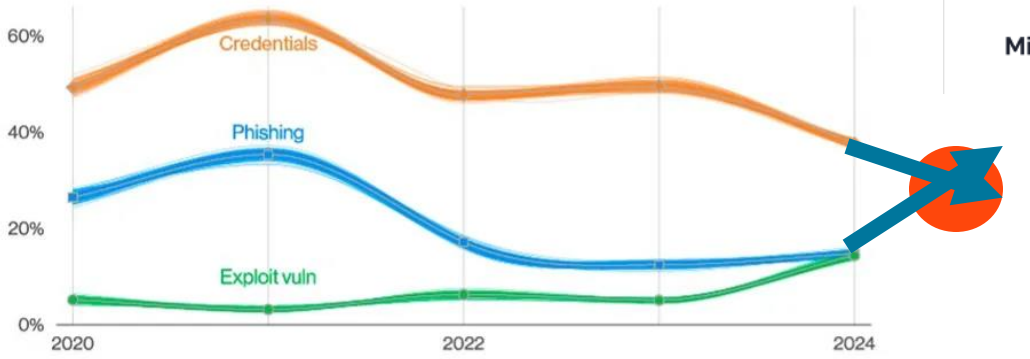
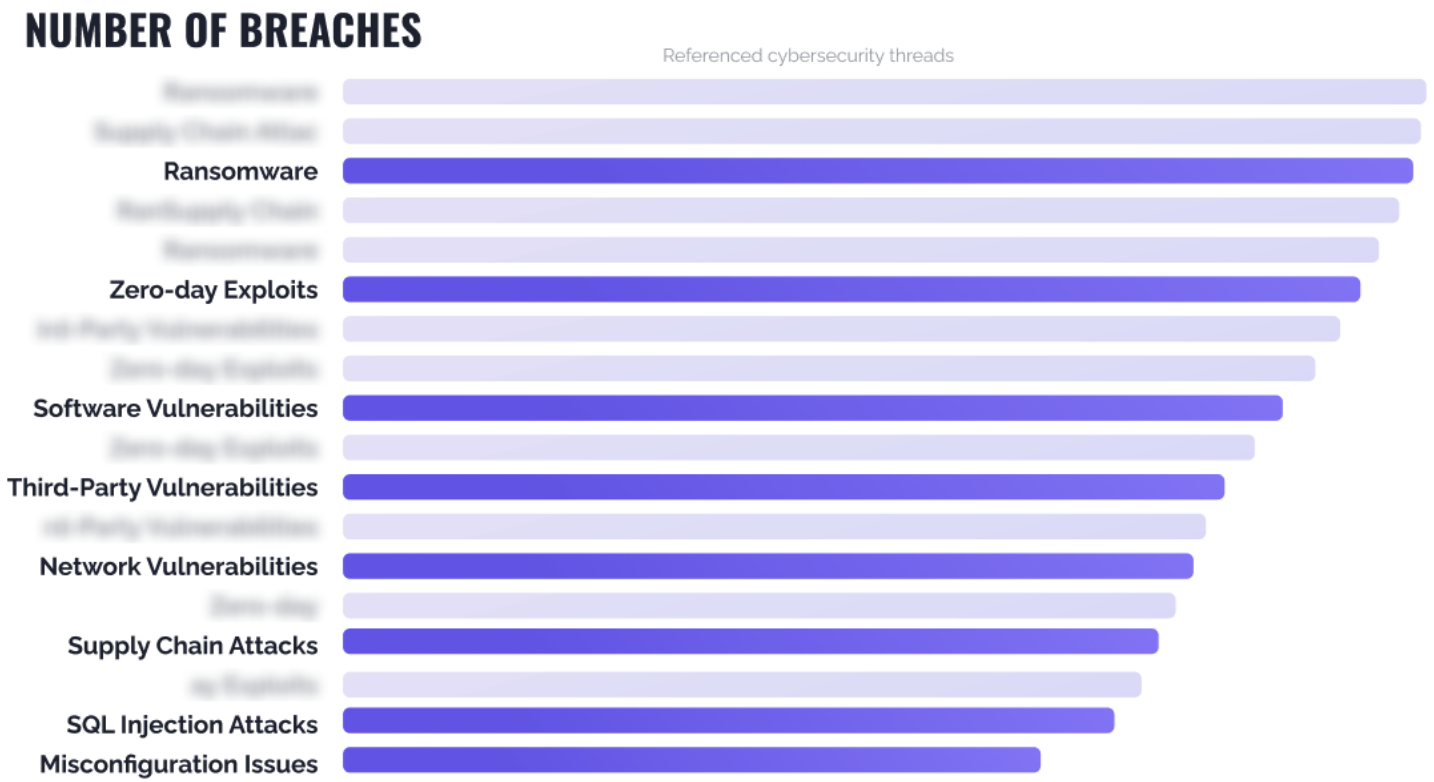


Figure 1. Select ways-in enumerations in non-Error, non-Misuse breaches (n=6,963)





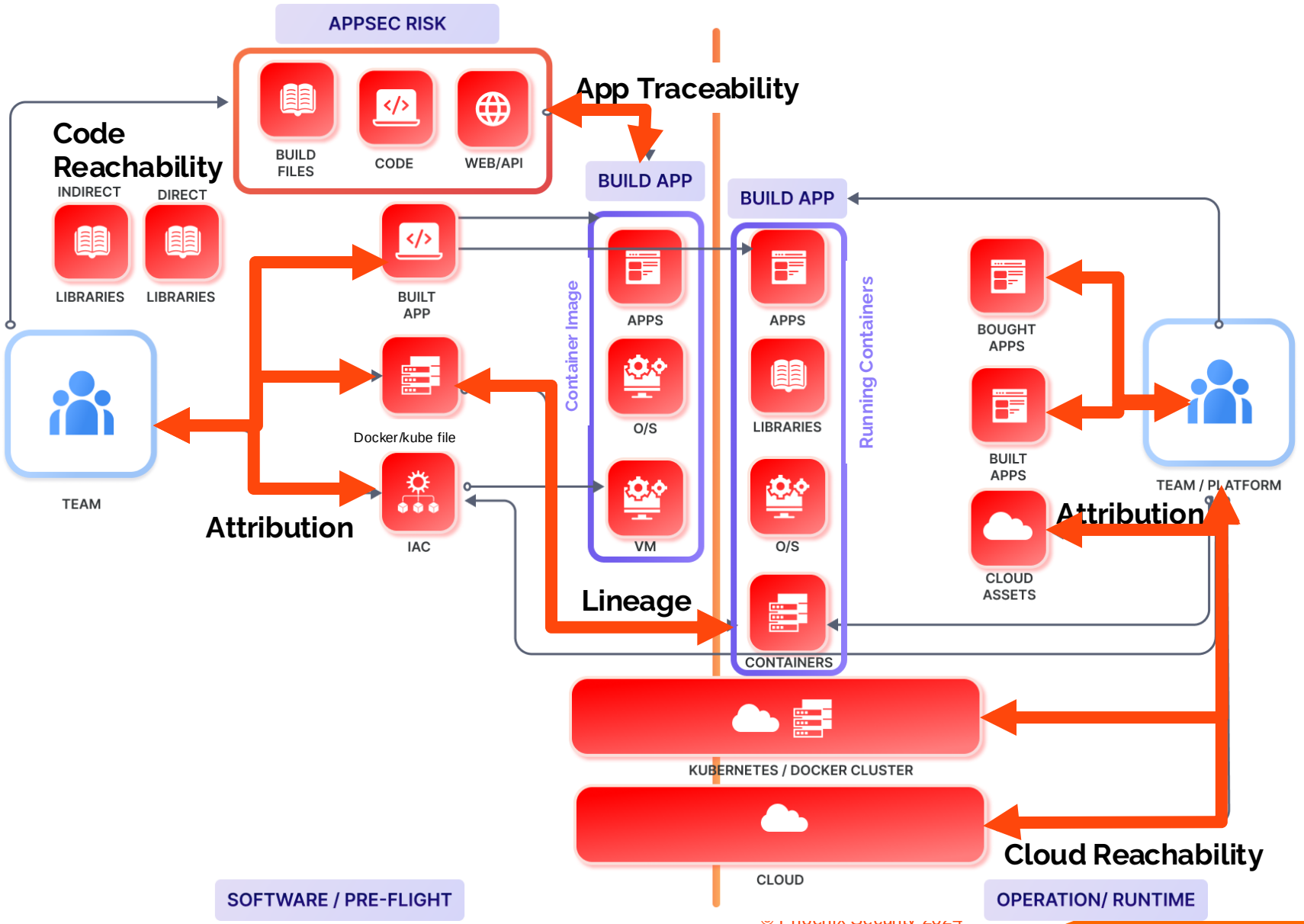
By 2025 the line will cross

Reference DBR 23

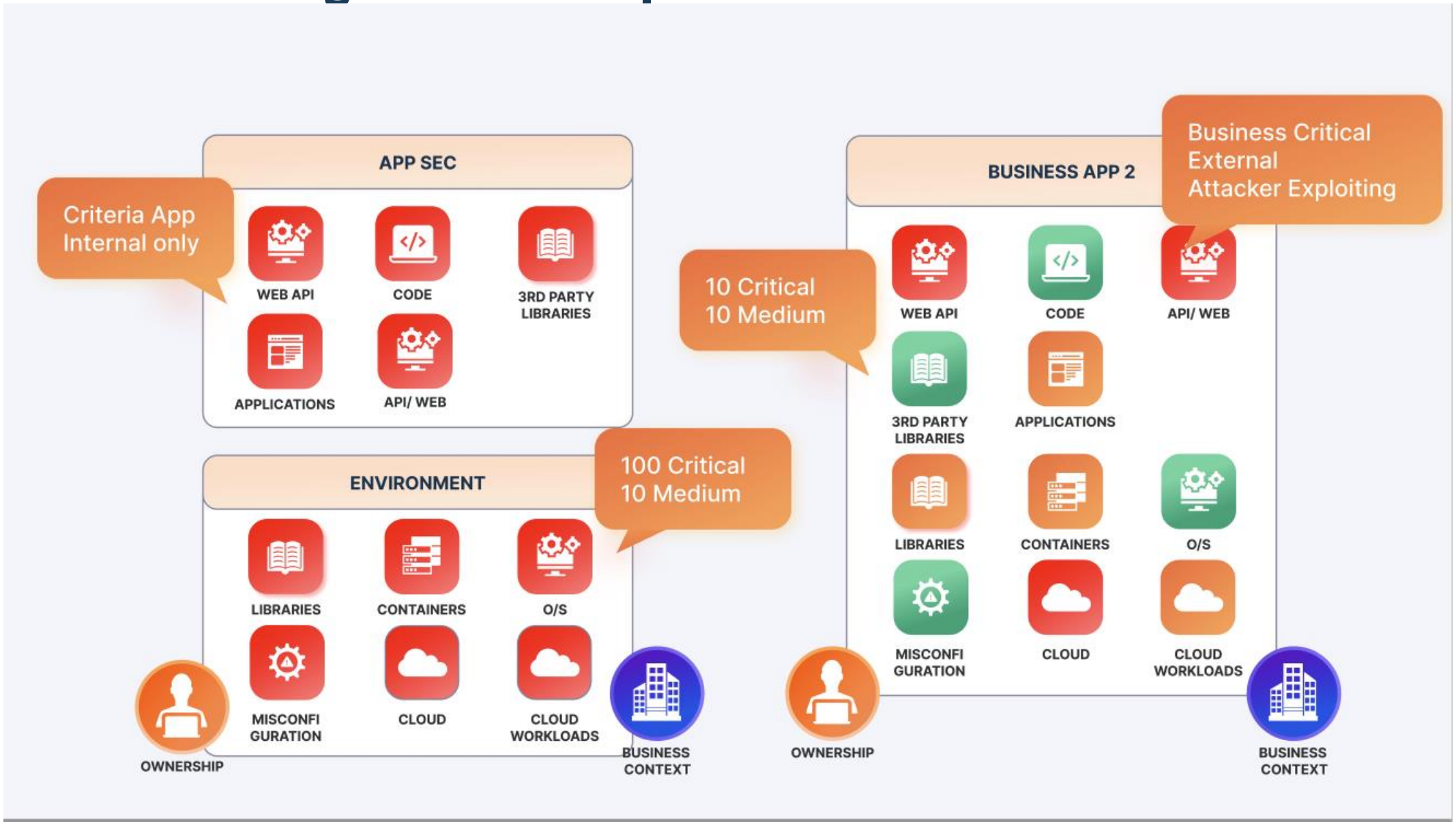
Bridging the gaps appsec and environment

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

- Attribution
- Lineage
- Traceability
- Code/Cloud Reachability

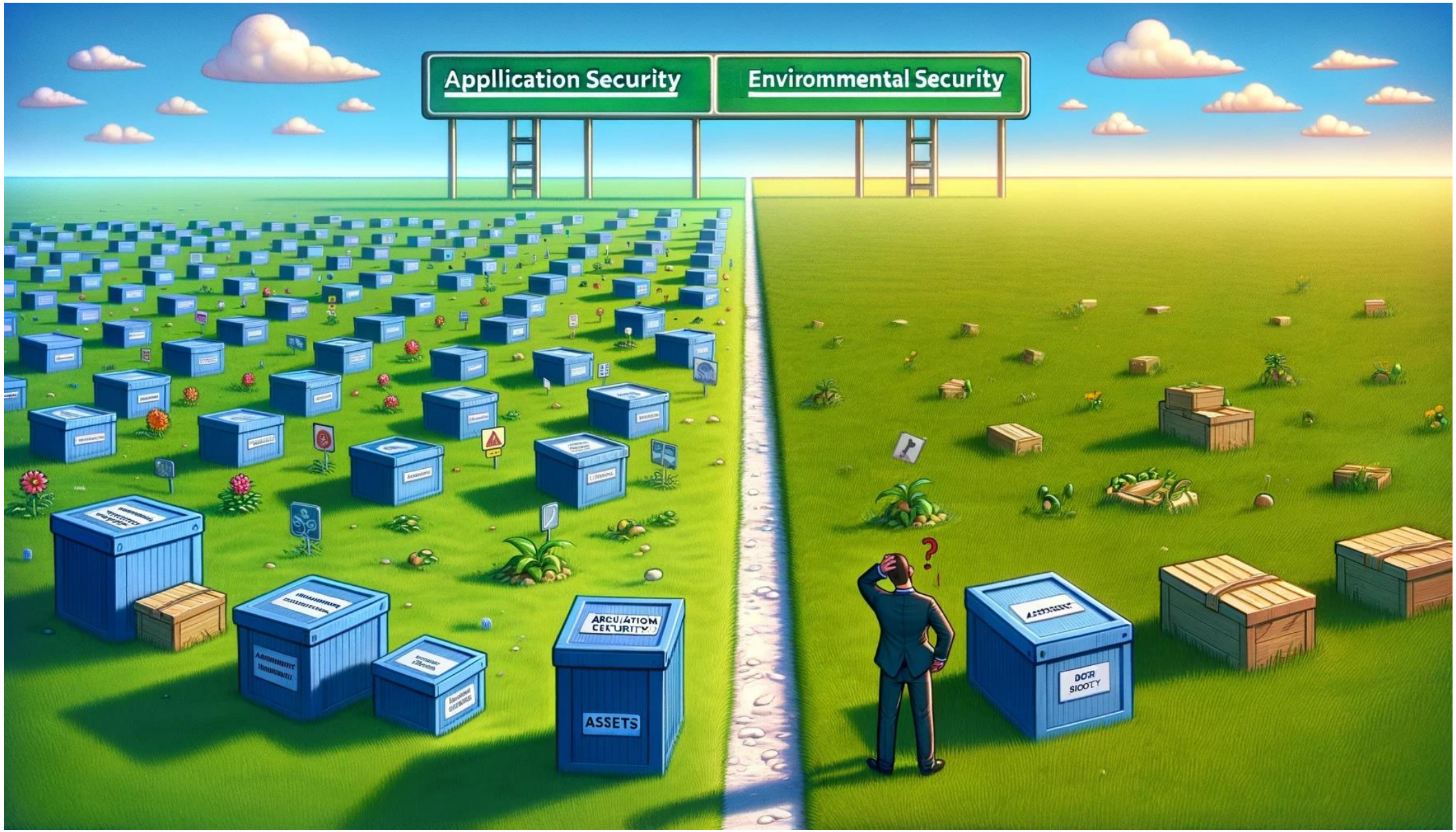


But we must recognize that the process are different

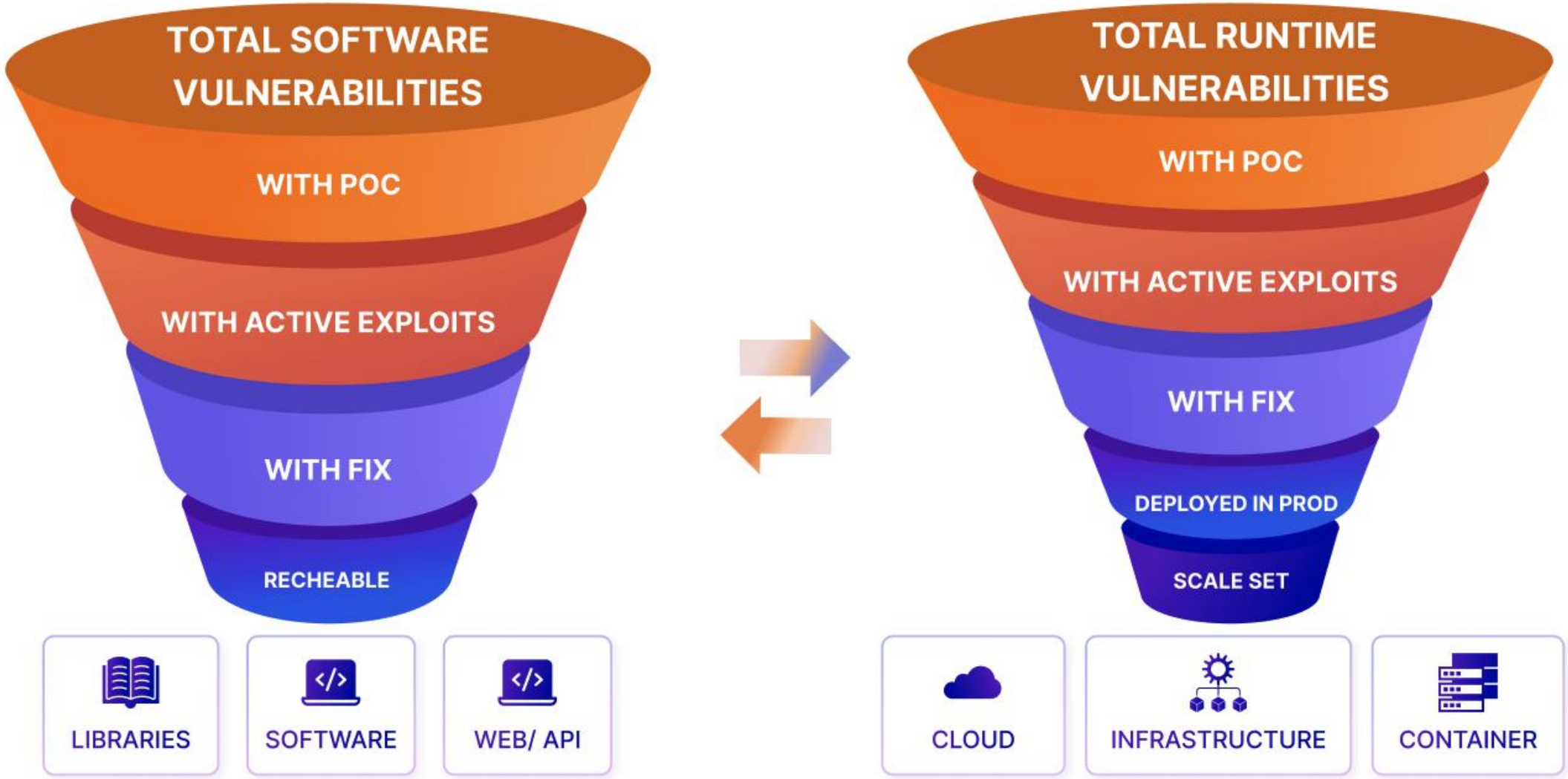


Scaling without an army
Data Driven Approach

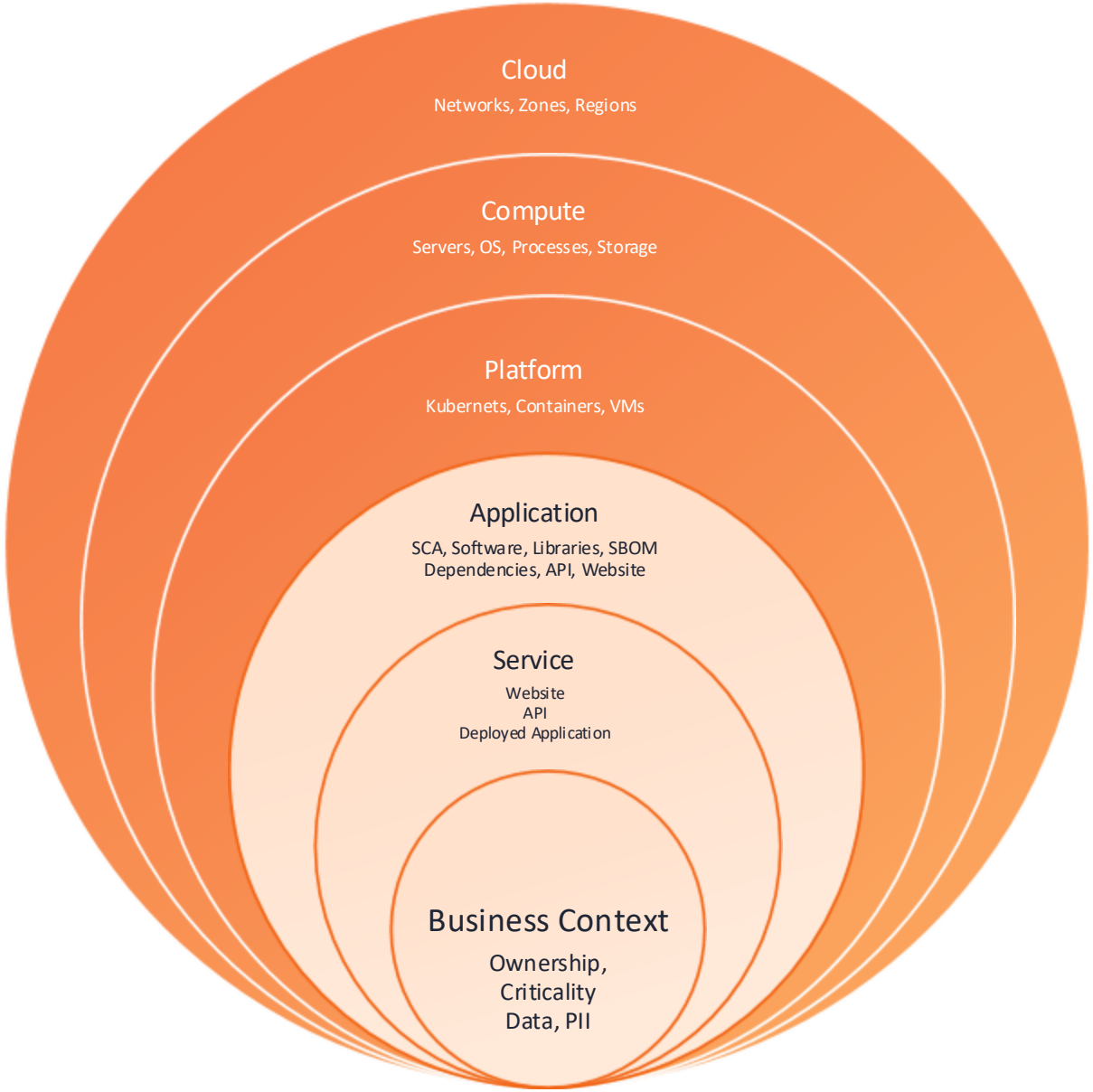
Assets and Risk, what are your assets, where is your risk?



Prioritization varies depending on the deployment

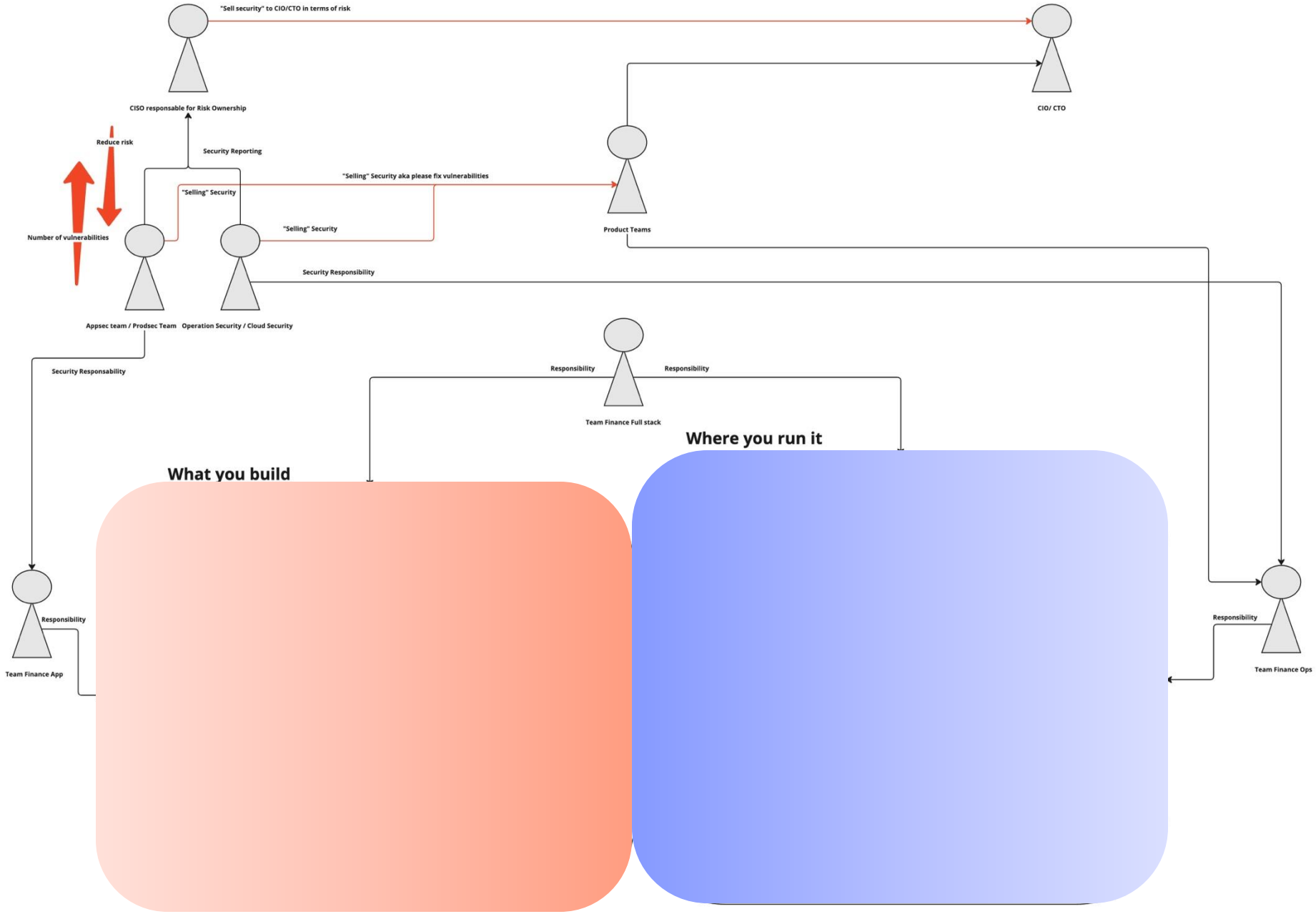


Code - Application Security / ASPM + ENVIRONMENT- Rumtime

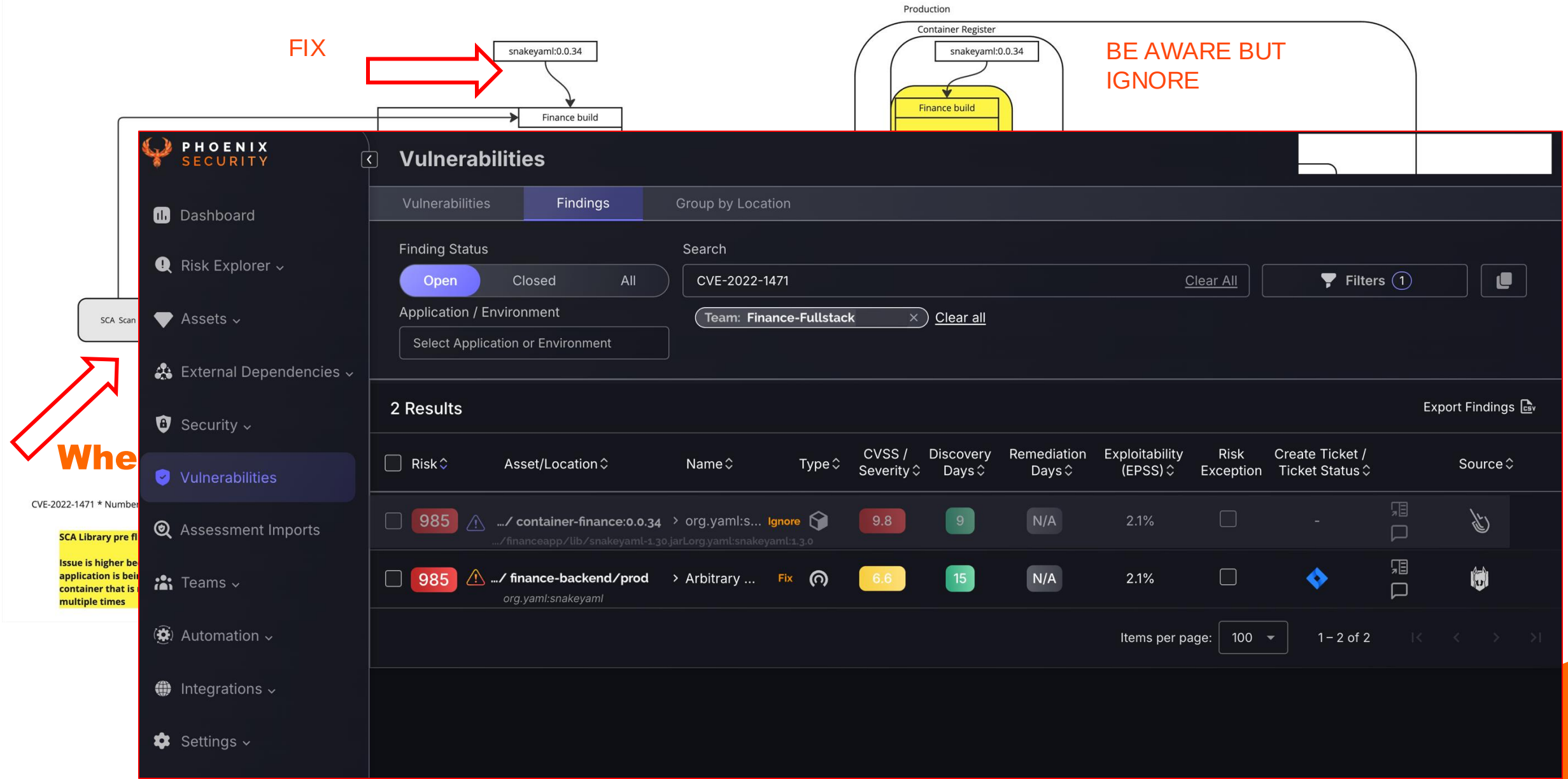


Line of communication

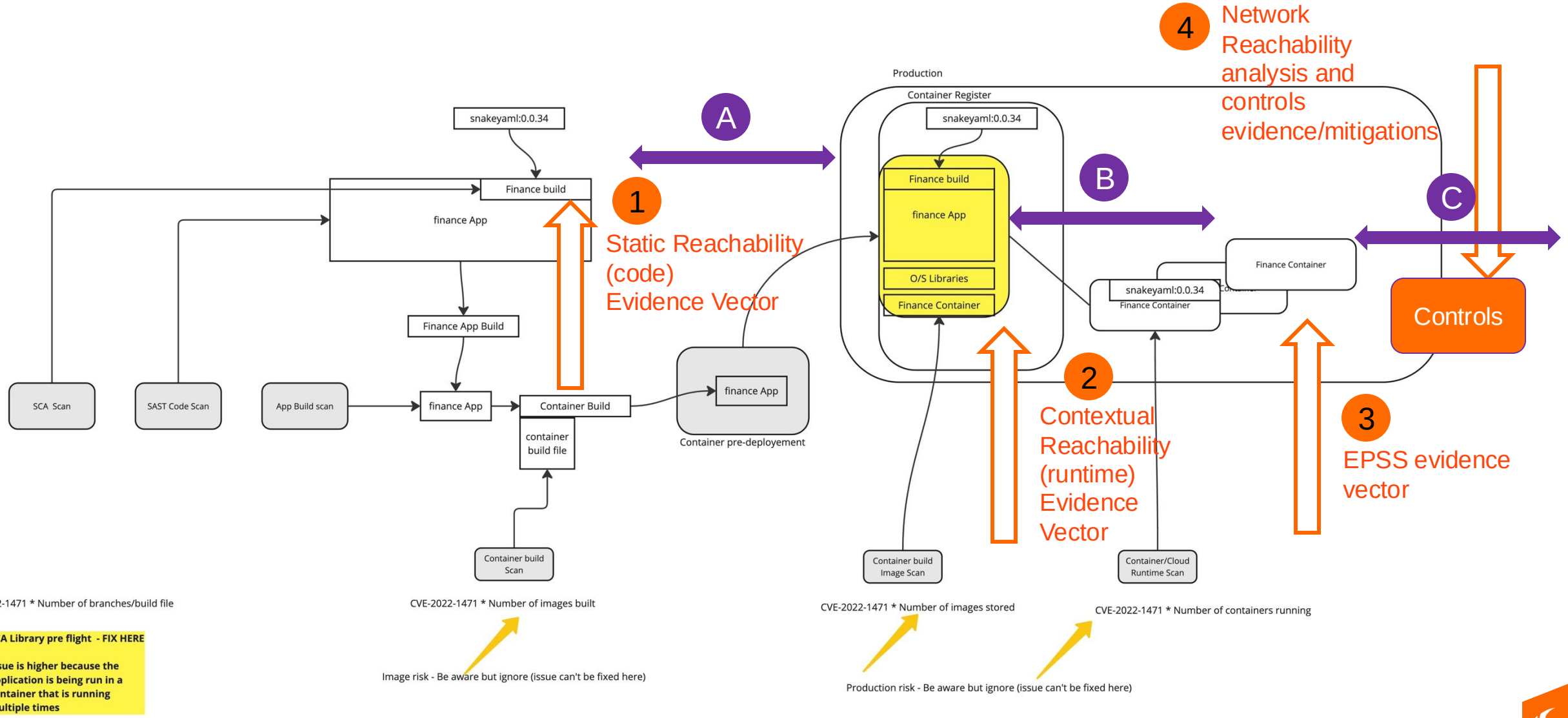
Line of communication are blurred, and attribution is king



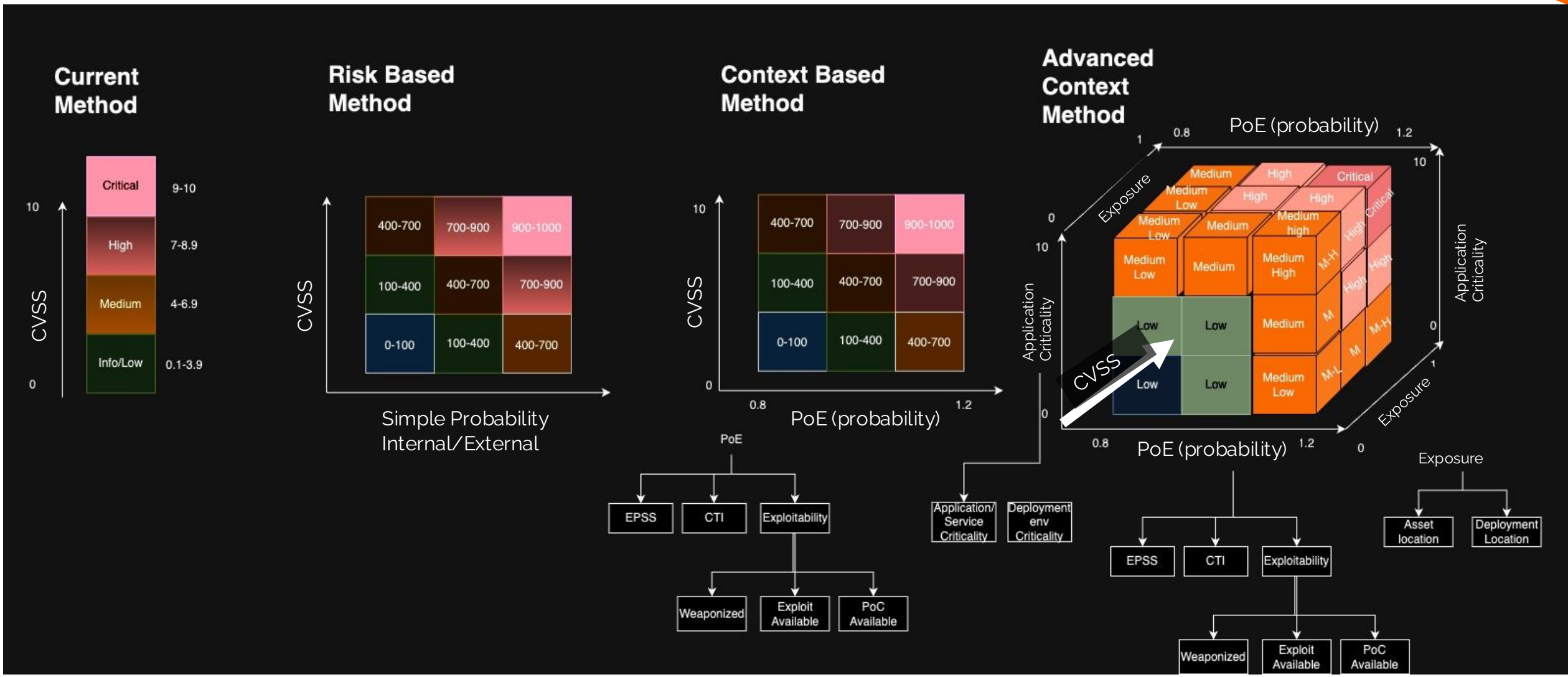
Real Case Scenario : Deduplicating Contextually Code and Libraries



Real Case Scenario : EPSS vs Static Reachability vs Runtime/Contextual Reachability



PHOENIX BRINGS OUT THE 4TH DIMENSION OF RISK



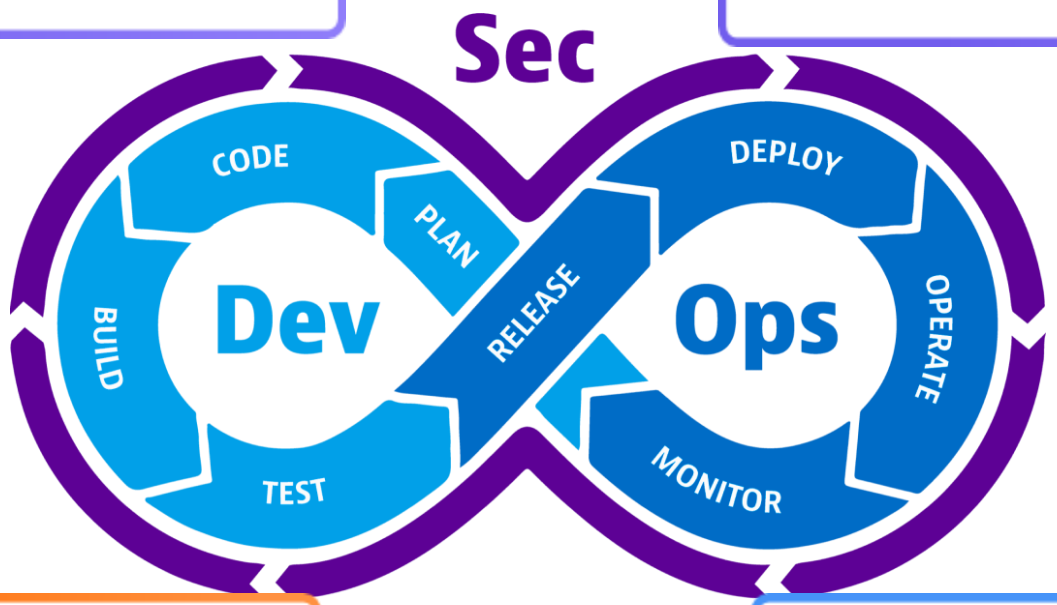
Shift Everywhere Connect business Security and Development

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



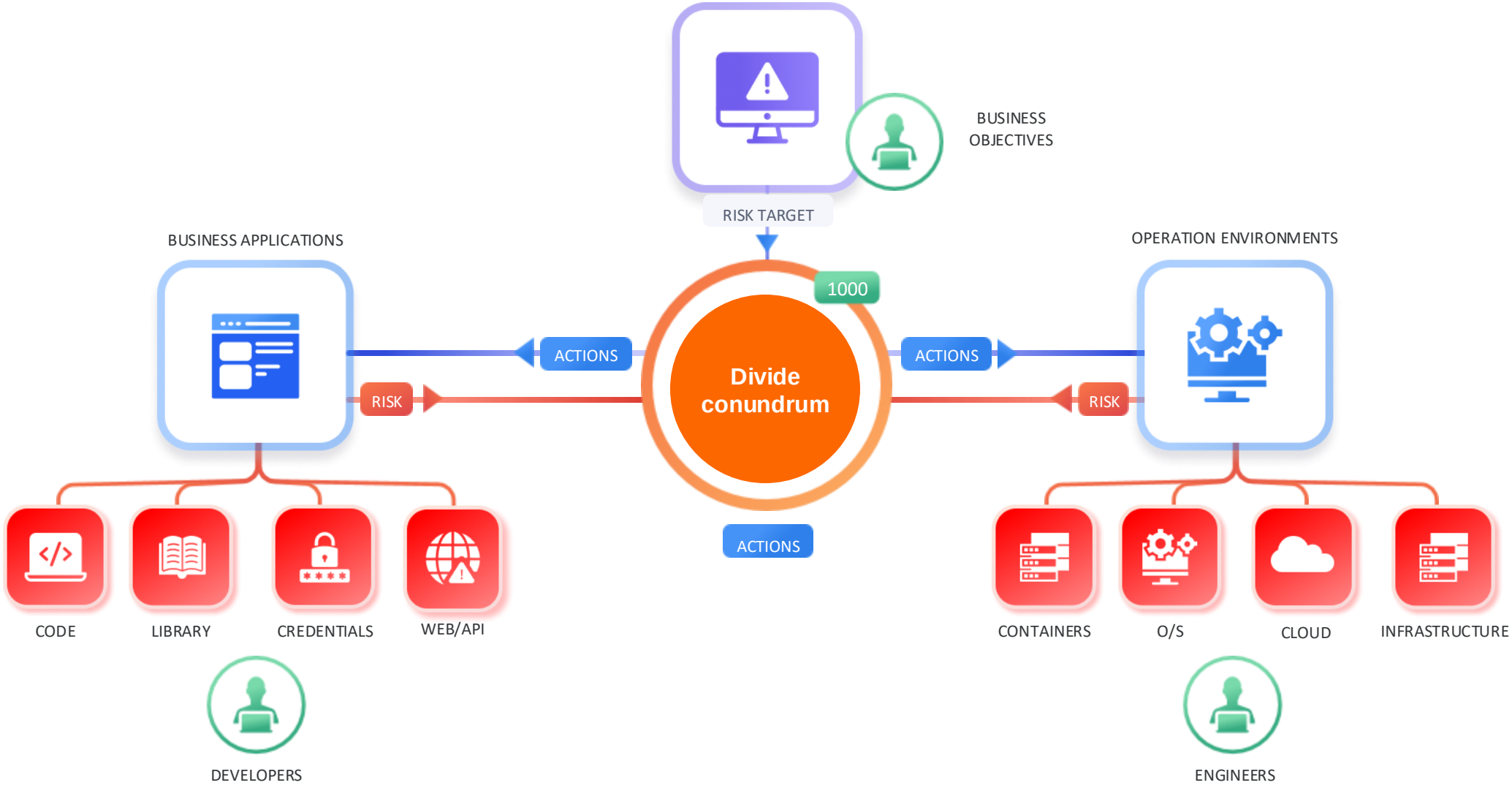
SHIFT LEFT (DevOps/DevSecOps)

- 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



SLOW DEFENDER

180-280 days

Average time to fix a vulnerability

DISCOVER

- Discover
- Scan
- Aggregate

PRIORITIZE

- Triage
- Correlate
- Prioritize
- Find Team/ Route
- Chase/Follow-Up

Exception Managment

ASSESS & ACT

- Plan/Schedule
- Follow-Up/Chase
- Resolve/Rescan
- Measure

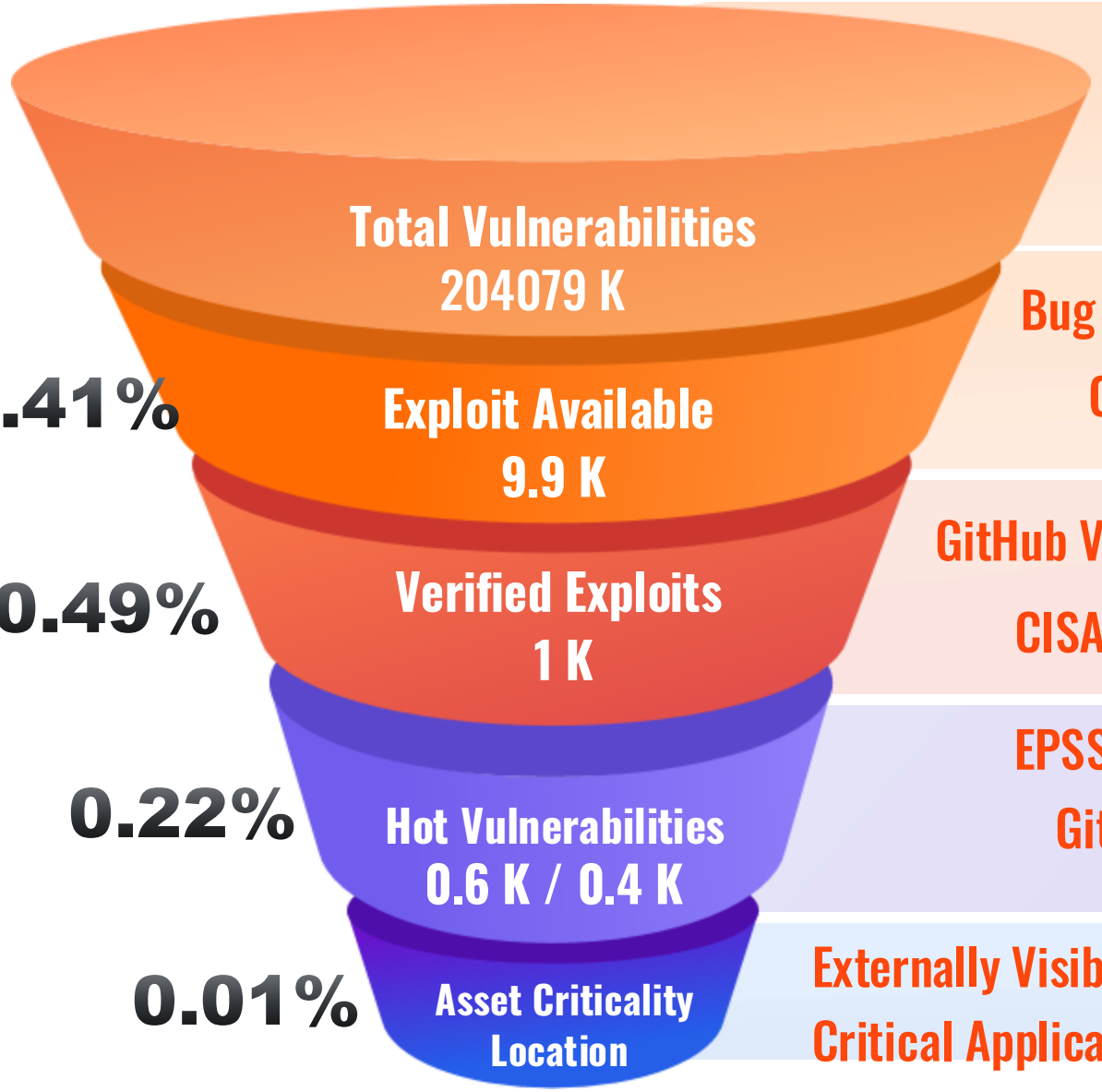
FAST ATTACKER

3-15 days

Average time to exploit a new vulnerability

- Discover
- Scan
- Prioritize
- Exploit
- Resolve

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%

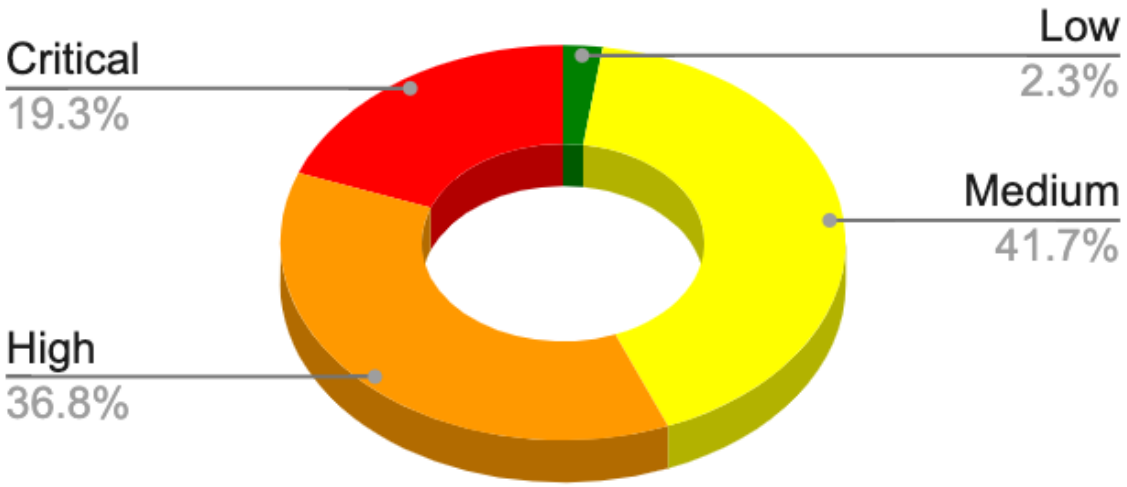
GitHub Active Exploit (0.40K) 0.22%

Externally Visible (0.14) ? 0.?%

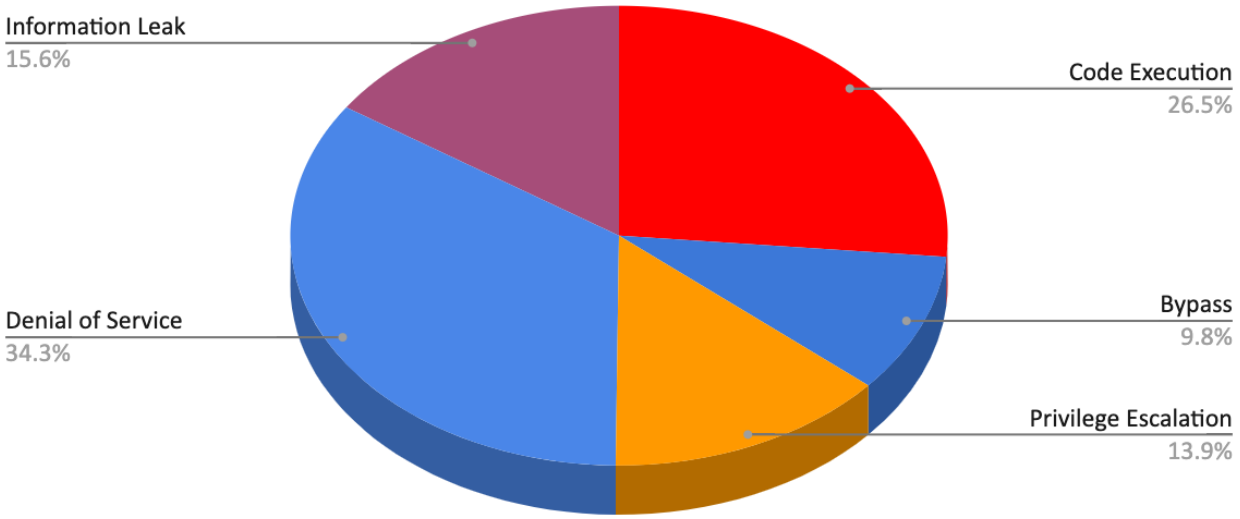
Critical Application

Prioritization

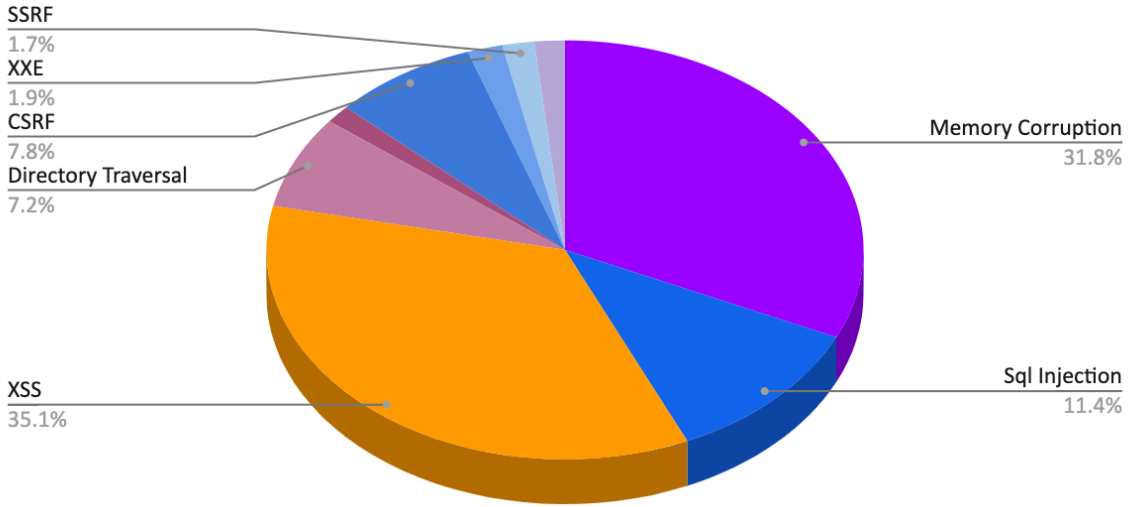
CVE Distribution

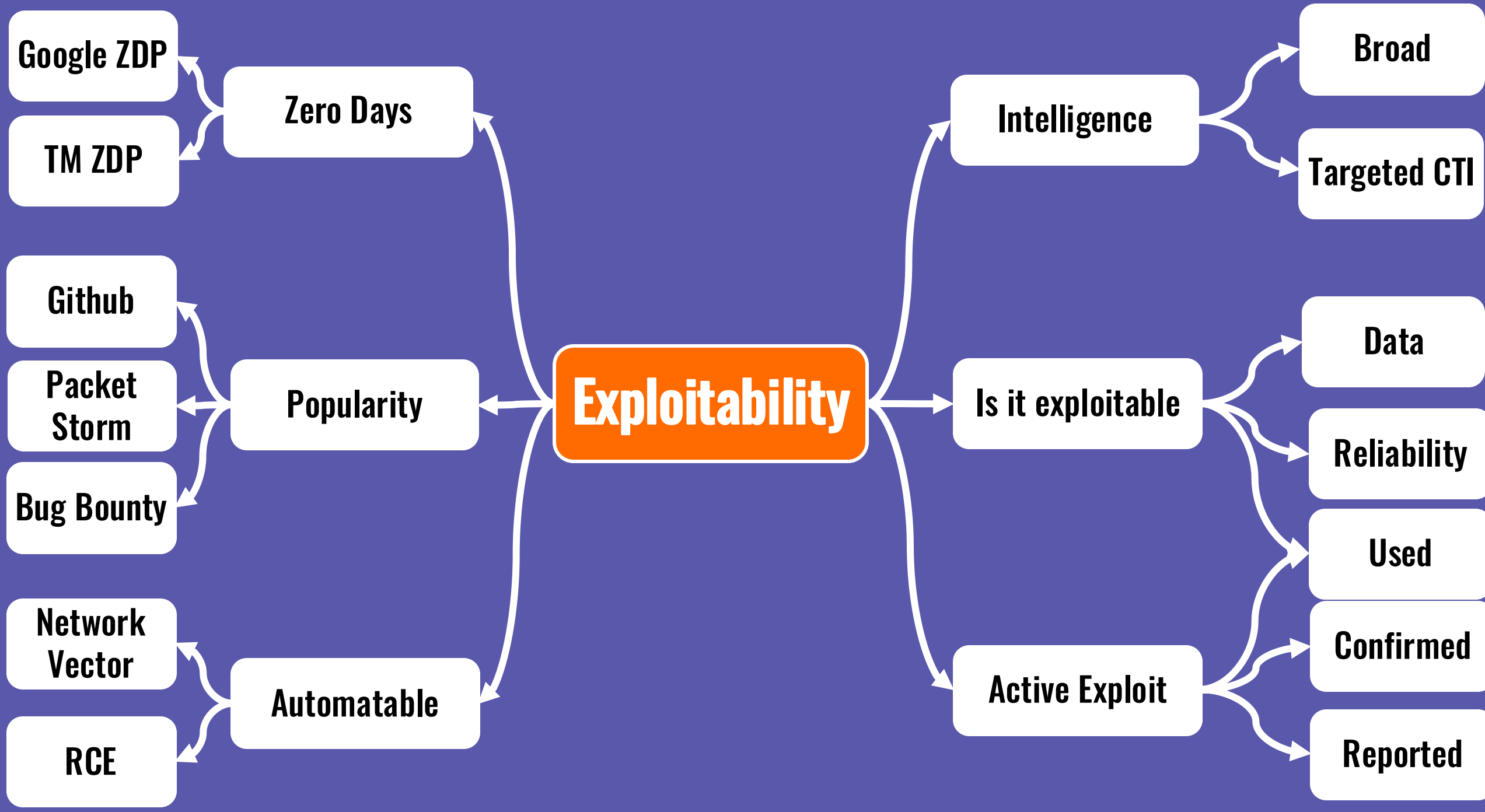


CVE Distribution by Effect

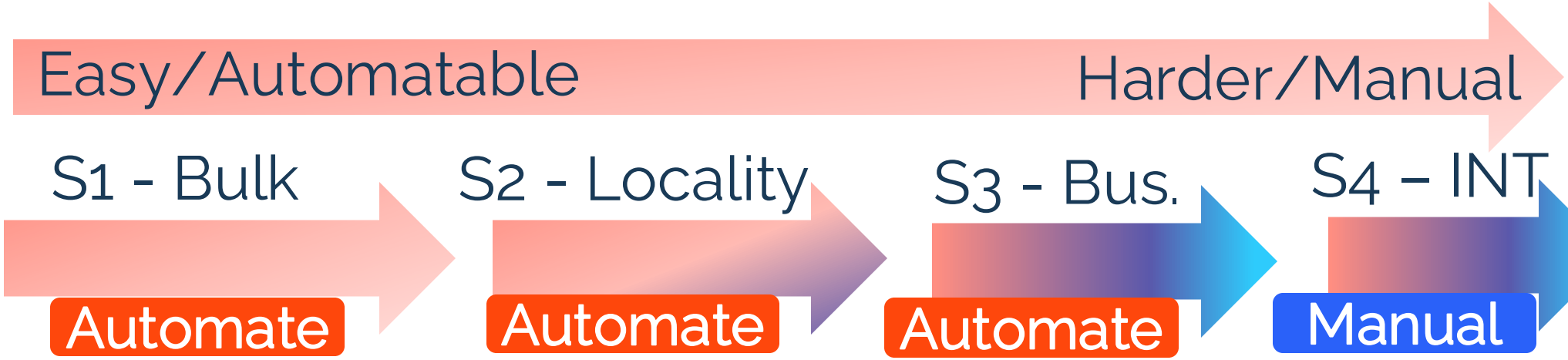


CVE Distribution by Type




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

Stages of triaging



Prioritize vulnerabilities

Is it reachable?

Is it critical?

Now?

Easy

Harder

- Exploitability
- Active Bounty
- Vector
- Reachability (code)

- Exploitability
- Location
- Reach (network)
- Attack Path

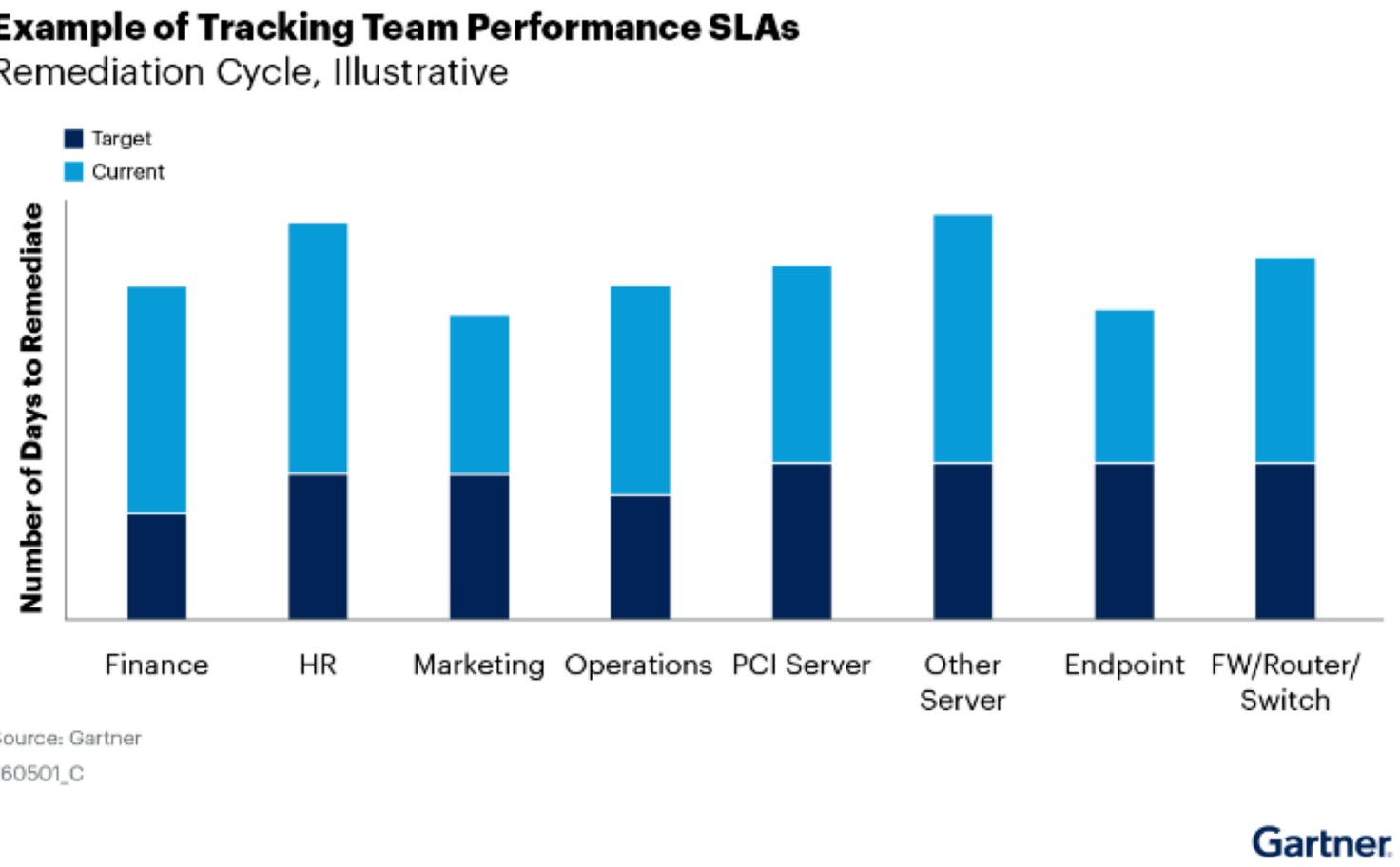
- Bus Criticality
- FAIR Analysis

- False Positive
- Deferred (project)
- Bus Rason

Using SLA is proven 100% unreachable objective

Actual Remedy

Objectives



Gartner

SLA Evolution

SLA Appetite

Low Maturity → **High Maturity**

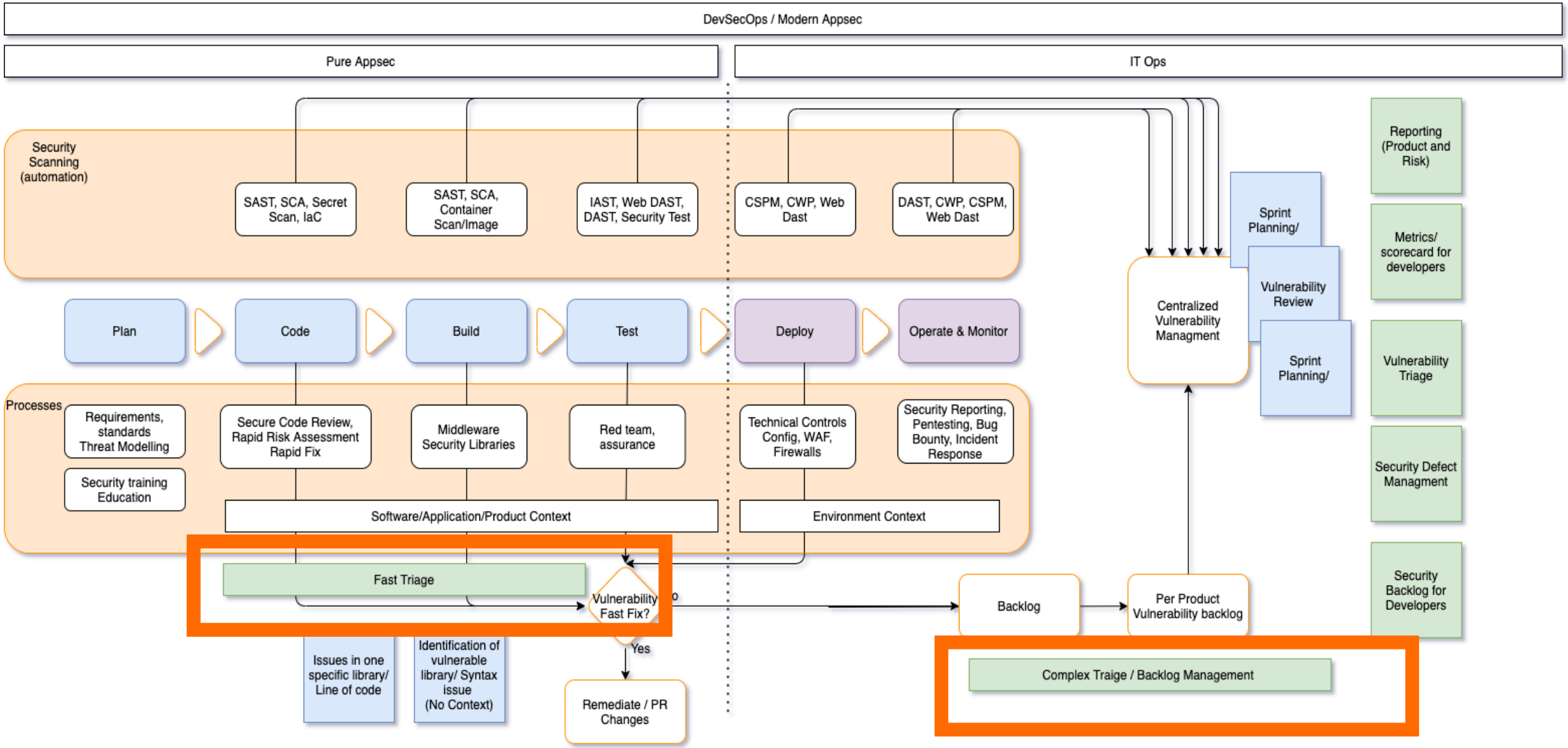
Severity SLA | Multi Severity SLA | Exposure SLA | Risk Based SLA

Simple to measure → **Complex to Measure**

Security OKR

SDLC and where scanner fit

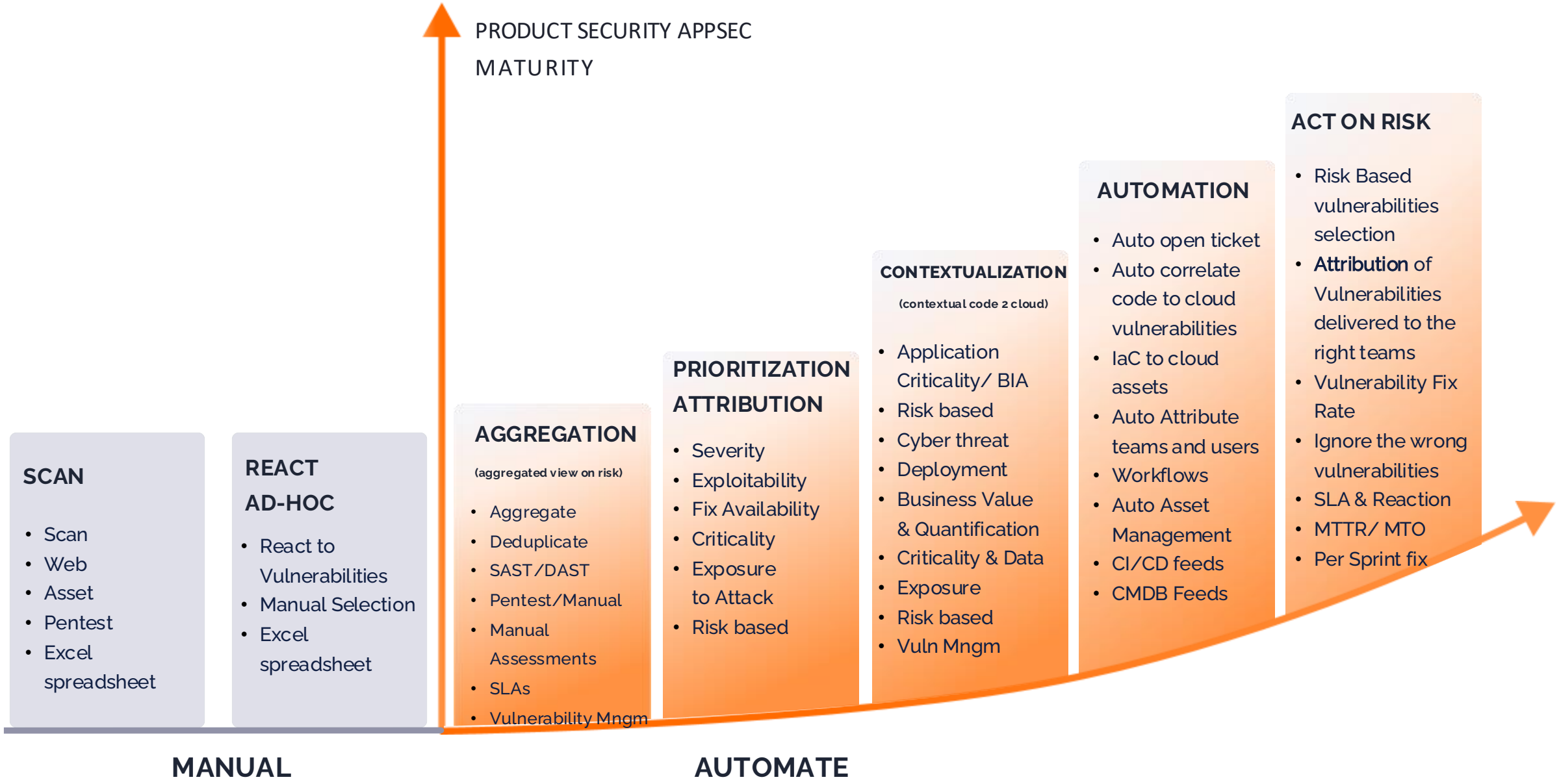
Modern security pipeline – Triage point



Vuln mngm framework

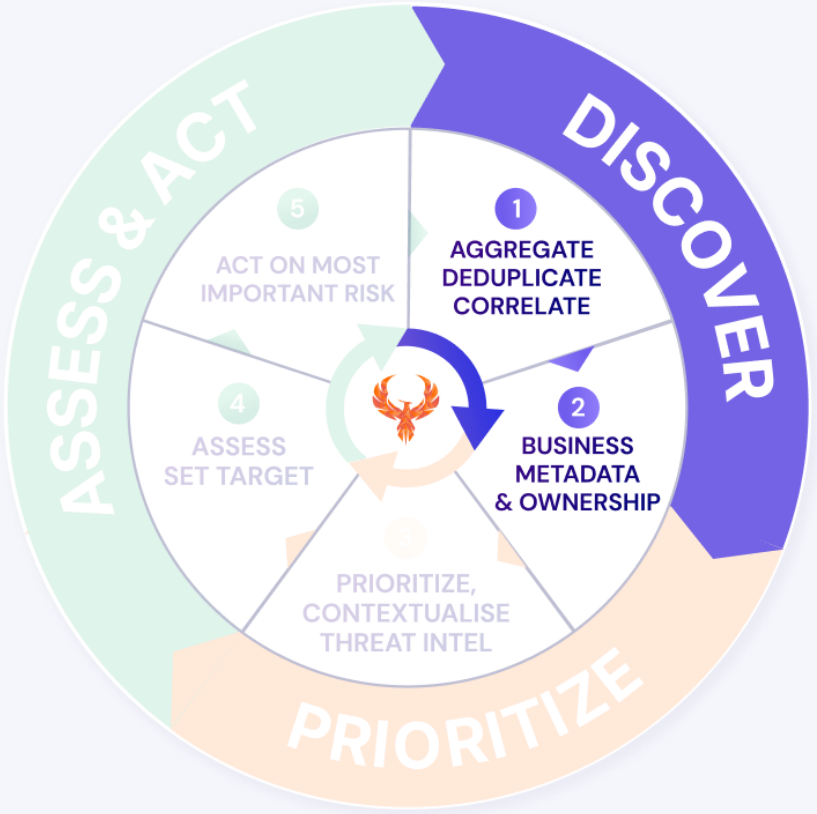
RISK is the answer

WHERE ARE YOU IN YOUR SOFTWARE SECURITY MATURITY JOURNEY?



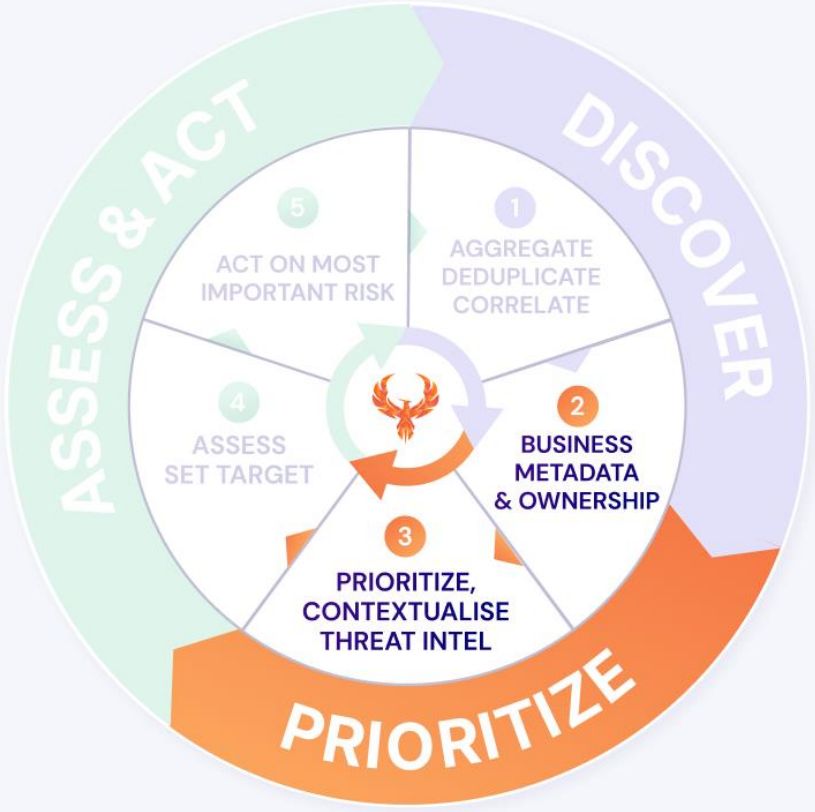
CONTEXTUALIZE PRIORITIZE | ACT ON RISK THAT MATTERS MOST

SCOPE, DISCOVER, AGGREGATE



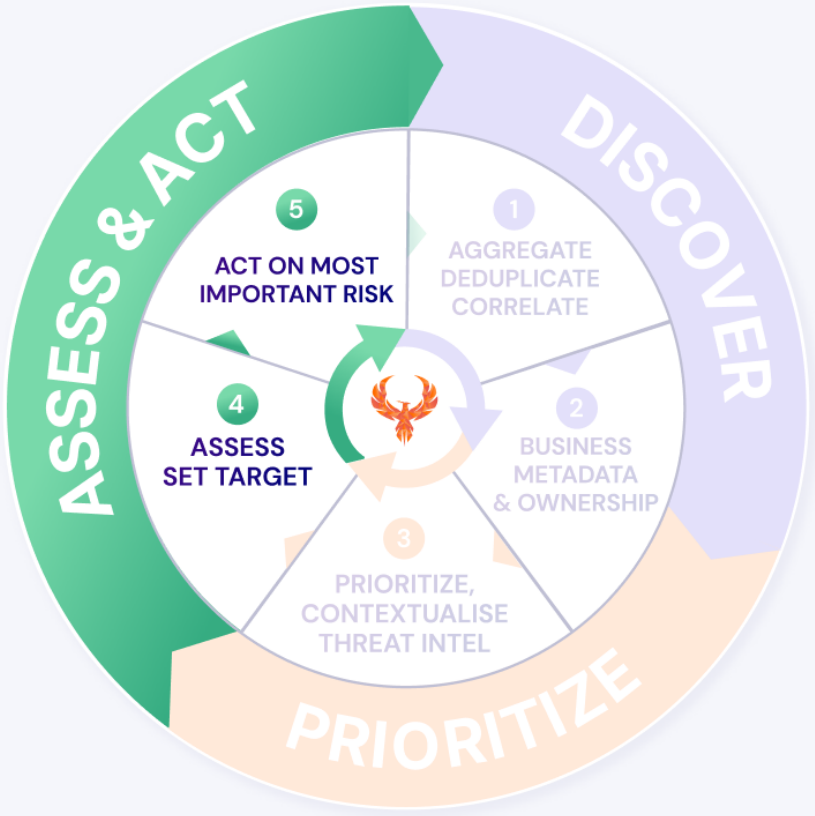
- AGGREGATE ALL THE DATA AND SET BASIC MEASUREMENT
- DISCOVER ASSET POSTURE
- SEGMENT THE ASSET BY BUSINESS AND ADD OWNERSHIP

PRIORITIZE



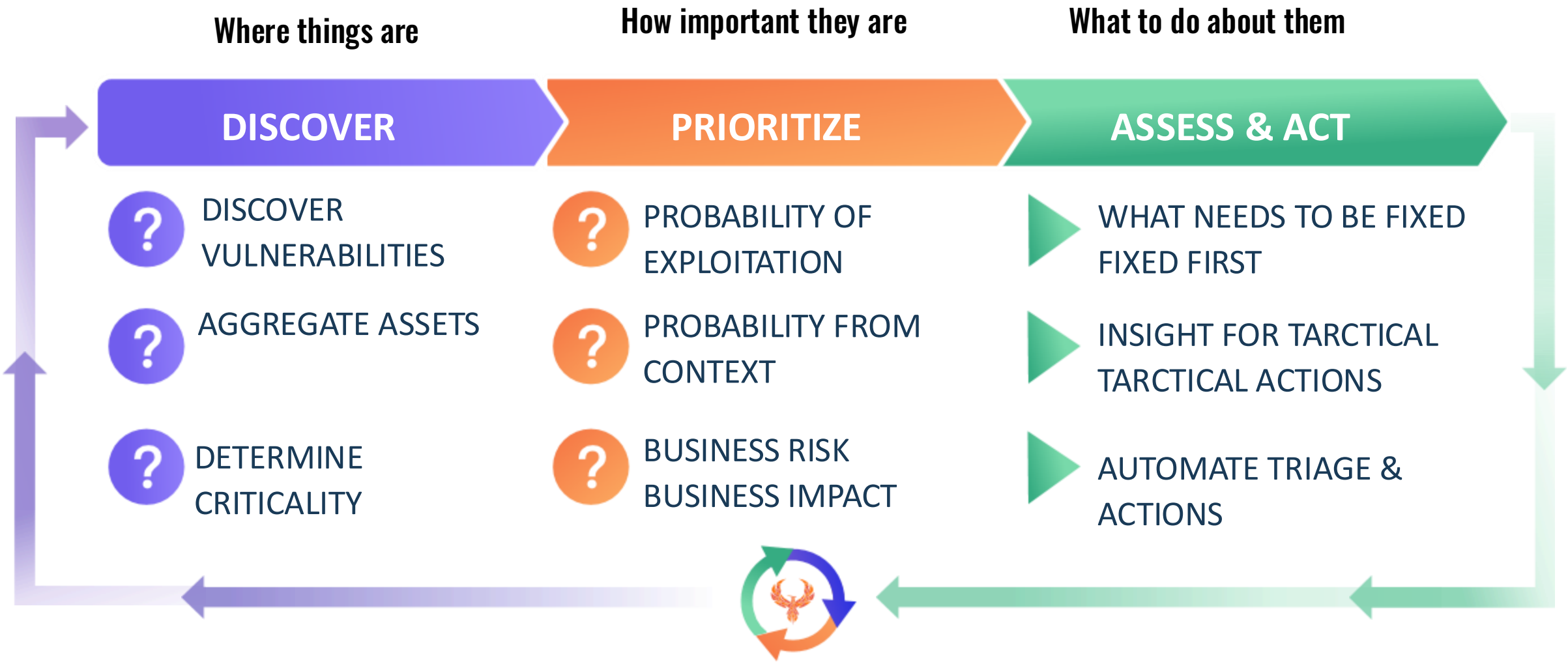
- PRIORITIZE BASED ON THREAT INTEL (EPSS)
- PRIORITIZE BASED ON CONTEXTUAL AND ASSET LOCATION
- PRIORITISE BASED ON BUSINESS CRITICALITY AND IMPACT

ACT



- ACT ON THE VULNERABILITIES THAT ARE MORE EXPLOITABLE
- SET RISK BASE TARGET AND ACT ON THE VULNERABILITIES TO REACH THE TARGET
- AUTOMATE THE OPENING OF TICKET, MEASURE MEAN TIME TO RESOLUTION

3 stages Of appsec



LEVEL	DETECTION	AGGREGATION/ ASSET MANAGMENT	PRIORITIZATION	ACTION	MEASUREMENT
M0	No Scan No Detection No Pentest	No Aggregation	No Prioritization	No action, ad-hoc reaction	No measurement No tracking
M1	Policy for Detection and scan Regular Pentest No SCA/ Library detection	Aggregate Vulnerabilities	Prioritization based on vulnerability severity	Regular review of vulnerability actions	Number of vulnerabilities
M2	Policy Regular Pen-test Ad-how Static analysis SAST Peer review	Aggregate vulnerabilities Aggregation of Assets	Prioritization based on SLA (severity)	Regular Review of vulnerability actions Regular Burn down of Vulnerabilities by SLA	Number of vulnerabilities SLA per criticality
M3	Policy Regular Pentest Automated Static analysis Automated SCA Peer review Vulnerability (O/S) Cloud assessment	Aggregate vulnerabilities Aggregation of Assets Asset contextualization (business)	Prioritization based on Risk SLA Prioritization based on Cyber threat intelligence and risk	Regular review of Backlog Regular Burn down of top vulnerabilities in the backlog	SLA per criticality SLA Risk based
M4	Policy Regular Pentest Automated Static analysis Automated SCA DAST WEB/ API Peer review Vulnerability (O/S) Container Scan Cloud assessment	Aggregate vulnerabilities Aggregation of Assets Asset contextualization (business) Contextual Location of assets Track the users / team operating on assets	Prioritization with Risk SLA Prioritization based on Cyber threat intel Prioritization based on business contextual information	Regular review of Backlog Regular Burn down of top vulnerabilities in the backlog Reporting to Business line based on Risk level, MTTR Feedback loop to dev on what to fix first.	Mean time to resolution Security balance SLA Risk based False positive/exception rate
M5	Policy Automated Pentest Static analysis SCA DAST WEB/ API Container Scan Peer review Vulnerability (O/S) Cloud assessment	Aggregate vulnerabilities Aggregation of Assets Self declared Asset contextualization (business) Self declared Contextual Location of assets/ Tag based Track the users / team operating on assets Track new assets automatically	Prioritization with RISK SLA, Prioritization based on TEAM OKR Prioritization based on Cyber threat intel, Prioritization based on business contextual information,	Regular review of Backlog Regular Burn down of top vulnerabilities in the backlog Reporting to Business line based on Risk level, MTTR, Burn-down rate Insights and strategic action based on the vulnerability observed Feedback loop to dev on what to fix first.	Mean time to resolution Users stories vs security Security backlog burndown SLA Risk based False positive/Exception rate Technology Insights Security OKR

LEVEL	DETECTION	AGGREGATION/ DEDUPLICATION	PRIORITIZATION	ACTION	MEASUREMENT
DSOMM MAPPING	TEST & VERIFICATION	TRIAGE	TRIAGE	CULTURE & ORG	MONITORING
SAMM V2 MAPPING	SECURITY TESTING	DEFECT MANAGEMENT	DEFECT MANAGEMENT	DEFECT MANAGEMENT	MEASURE & IMPROVE STREAM B
M0	No Scan No Detection No Pentest	No Aggregation	No Prioritization	No action, ad-hoc reaction	No measurement No tracking
M1	Policy mandating scanning requirements / Secure SDLC Regular Pentest / External Scan No SCA/ Library detection	Aggregate Vulnerabilities in entral place	Prioritization based on vulnerability severity	Fix based on severity	Number of vulnerabilities
M2	Policy mandating scanning requirements / Secure SDLC Regular Pen-test / External Scan Ad-how Static analysis Infra Vulnerability - L1 (O/S - Endpoint, Installed Apps) SAST - Static Code Analysis or SCA	Aggregate vulnerabilities per business application Aggregation of Assets Deduplication - L0 - Manual	Prioritization based on vulnerability severity Prioritization based on SLA (severity)	Fix based on severity Triage & Assess	Number of vulnerabilities SLA per criticality
M3	Policy mandating scanning requirements / Secure SDLC Regular Pen-test / External Scan Automated Static code analysis Infra Vulnerability - L2 (Image Scanning, O/S - Servers, O/S - Endpoint, Installed Apps, Network Scanning) Automated Library assessment / OSS- SCA Code Peer review	Aggregate vulnerabilities per business application Aggregation of Assets Asset contextualization (business) Deduplication L1 - Automated - (Assets Dedup, CVE Dedup)	Prioritization based on vulnerability severity Prioritization based on Risk/ Risk Based SLA Prioritization based on Cyber threat intelligence	Fix based on Risk/ SLA Triage & Assess / Exception management - L1 (False Positives)	Number of vulnerabilities SLA per criticality

LEVEL	DETECTION	AGGREGATION/ DEDUPLICATION	PRIORITIZATION	ACTION	MEASUREMENT
DSOMM MAPPING	TEST & VERIFICATION	TRIAGE	TRIAGE	CULTURE & ORG	MONITORING
SAMM V2 MAPPING	SECURITY TESTING	DEFECT MANAGEMENT	DEFECT MANAGEMENT	DEFECT MANAGEMENT	MEASURE & IMPROVE STREAM B
M4	Policy mandating scanning requirements / Secure SDLC Bug Bounty/ Pentest Automated Static analysis Automated SCA Automate TEST WEB/ DAST API Assessment Code Peer review Infra Vulnerability - L3 (Image Scanning, O/S - Servers, O/S - Endpoint, Installed Apps, Network Scanning) Container Scan Cloud assessment/ IaC	Aggregate vulnerabilities per business application Aggregation of Assets Asset contextualization (business) Contextual Location of assets Deduplication L2- Automated - (Assets Dedup, CVE Dedup, Contextual Deduplication) Track the users / team operating on assets	Prioritization based on vulnerability severity Prioritization with Risk/ Risk based SLA Prioritization based on Cyber threat intel Prioritization based on business contextual information	Fix based on Risk/ SLA Triage & Assess / Triage & Schedule (sprint planning) - Backlog management Exception management - L2 (Mitigation controls, False Positives)	SLA per criticality SLA Risk based Mean time to resolution Security balance False Positive/Exception rate Security insights
M5	Policy mandating scanning requirements / Secure SDLC Automated Pentest Bug Bounty/Pentest Automated Static Analysis Automated SCA Automated DAST WEB/ Automated API Container Scan / Preflight Container Build Code Peer review Infra Vulnerability - L3 (Image Scanning, O/S - Servers, O/S - Endpoint, Installed Apps, Network Scanning) Cloud assessment/ Automated IaC	Aggregate vulnerabilities Aggregation of Assets Deduplication L3 - (Assets Dedup, CVE Dedup, Automated Function SCA-SAST, Contextual Deduplication) Self Declared Asset/ Centralization of assets declaration Contextualization (business) with Business Impact Self Declared Contextual Location of assets/ Tag based Track the users / team operating on assets Track new assets automatically	Prioritization based on vulnerability severity Prioritization with RISK/ Risk based SLA, Prioritization based on TEAM OKR Prioritization based on Cyber threat intel, Prioritization based on Contextual information Prioritization based on business contextual information,	Fix based on Risk/ SLA Triage & Assess / Triage & Schedule (sprint planning) - Backlog management Exception management - L3 (Mitigation controls, False Positives, Risk Acceptance)	Mean time to resolution/ MTTR Users Stories vs Security Security backlog burn-down SLA Risk based , False Positive/Exception rate Technology Insights Security OKR Security Insights Build vs Fix stories Localised insights (per business application)

Detection Maturity Model

LEVEL	DETECTION	AGGREGATION/ DEDUPLICATION	PRIORITIZATION	ACTION	MEASUREMENT
M0	M1	M2	M3	M4	M5
	• Policy mandating scanning requirements / Secure SDLC • Regular Pentest / External Scan • No SCA/ Library detection	• Policy mandating scanning requirements / Secure SDLC • Regular Pen-test / External Scan • Ad-how Static analysis • Infra Vulnerability - L1 (O/S - Endpoint, Installed Apps) • SAST - Static Code Analysis or SCA	• Policy mandating scanning requirements / Secure SDLC • Regular Pen-test / External Scan • Automated Static code analysis Infra Vulnerability - L2 (Image Scanning, O/S - Servers, O/S - Endpoint, Installed Apps, Network Scanning) • Automated Library assessment / OSS- SCA Code Peer review	• Policy mandating scanning requirements / Secure SDLC Bug Bounty/ Pentest • Automated Static analysis Automated SCA • Automate TEST WEB/ DAST API • Assessment Code Peer review Infra • Vulnerability - L3 (Image Scanning, O/S – • Servers, O/S - Endpoint, Installed Apps, Network Scanning) • Container Scan Cloud assessment/ IaC	Policy mandating scanning requirements / Secure SDLC Automated Pentest Bug Bounty/Pentest Automated Static Analysis Automated SCA Automated DAST WEB/ Automated API Container Scan / Pre-flight Container Build Code Peer review Infra Vulnerability - L3 (Image Scanning, O/S - Servers, O/S - Endpoint, Installed Apps, Network Scanning) Cloud assessment/ Automated IaC

Metrics

LEVEL	DETECTION	AGGREGATION/ DEDUPLICATION	PRIORITIZATION	ACTION	MEASUREMENT
M0	M1	M2	M3	M4	M5
	• Number of vulnerabilities/ Vulnerability Severity	• Number of vulnerabilities (appsec or infra vuln management) • SLA per vulnerability severity (aka criticality) • Fix only Critical Risk • Fix rate	• SLA per criticality • SLA Risk based Vulnerability Debt (number of fixes vs number of vuln introduced) • From Ticket to Patch Management Statistics/ Mean time to Resolution • From Vulnerability to remediation (mean time to Fix) • Integration of vulnerability issue into development processes • Fix Contextualize (Critical - Medium) Vulnerability Management System Fix rate per repo/ product	• Like M3 • False Positive/Exception rate • Security insights • Fix by contextual risk (Critical - Medium) • Reproducible Defects • Advanced visualization of defect? • Fix rate per repo/ product • Fix rate per team • False positive rate	• Like M4 • Plus: • Mean time to resolution/MTTR • Users Stories vs Security Security • backlog burndown • Vulnerability Debt (number of fixes vs number of vuln introduced) • SLA Risk based , • False Positive/Exception rate • Technology Insights • Security OKR • Security Insights • Localized insights (per business application)

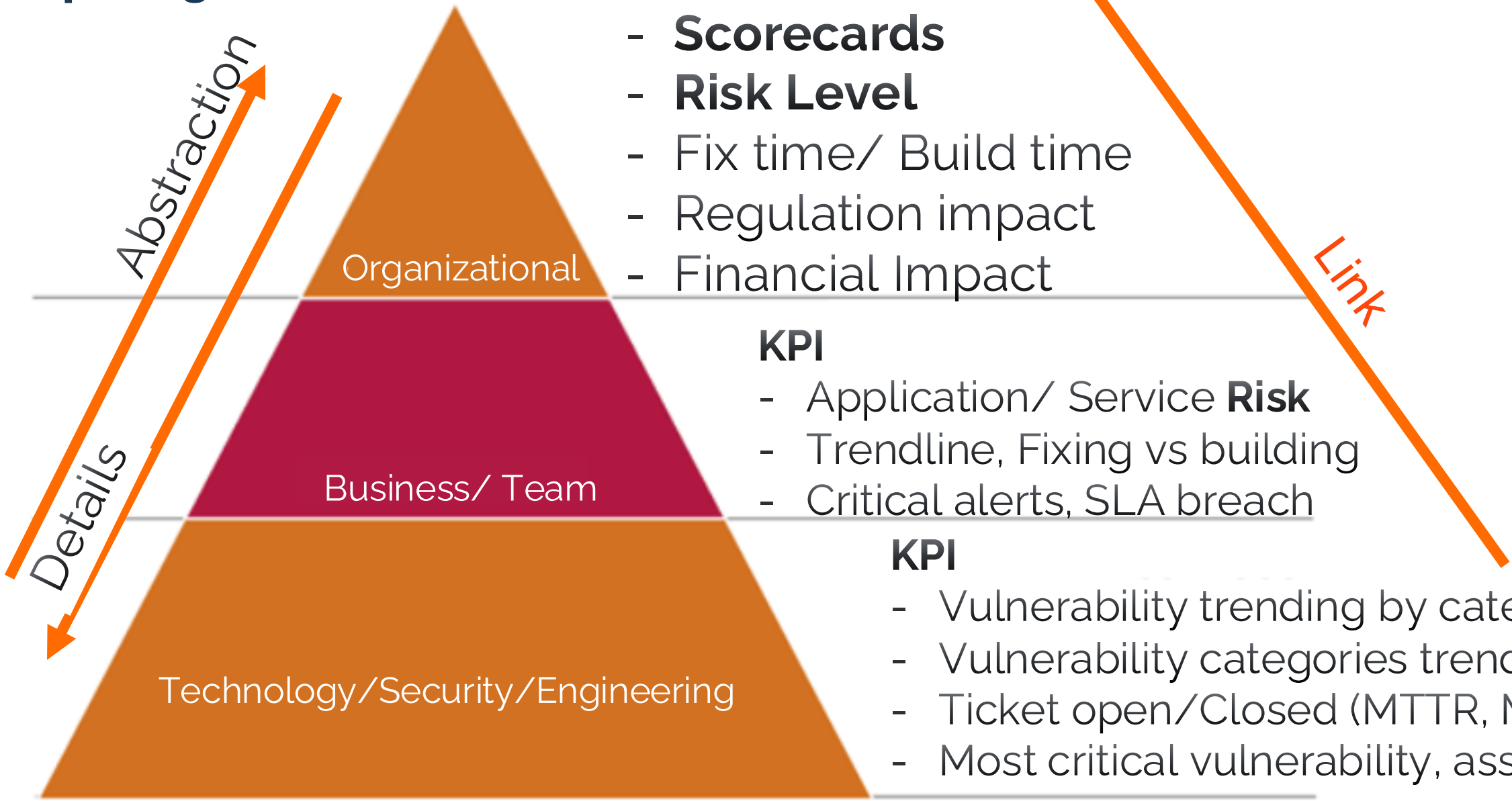
No measurement
No tracking

LEVEL	DETECTION / TESTING	AGGREGATION	PRIORITIZATION	VULNERABILITY ACTION	VULNERABILITY PROCESS	MEASUREMENT
DSOMM MAPPING	TEST & VERIFICATION	TRIAGE	TRIAGE	TRIAGE	CULTURE & ORG	MONITORING
SAMM V2 MAPPING	SECURITY TESTING	DEFECT MANAGEMENT	DEFECT MANAGEMENT	DEFECT MANAGEMENT	DEFECT MANAGEMENT	MEASURE & IMPROVE STREAM B
M0	• No Scan • No Detection • No Pentest	• No Aggregation	• No Prioritization	• Fix random	• No Action	• No measurement No tracking
M1	• Policy mandating scanning requirements / Secure SDLC • Regular Pentest / External Scan • No SCA/ Library detection	• Aggregate Vulnerabilities in entral place	• Prioritization based on vulnerability severity	• Fix based on severity	• Reactive and Regular review of vulnerability actions	• Number of vulnerabilities/ Vulnerability Severity
M2	• Policy mandating scanning requirements / Secure SDLC • Regular Pen-test / External Scan • Ad-how Static analysis • Infra Vulnerability - L1 (O/S - Endpoint, Installed Apps) • SAST - Static Code Analysis or SCA	• Aggregate vulnerabilities per business application • Aggregation of Assets • Deduplication - L0 - Manual	• Prioritization based on vulnerability severity • Prioritization based on SLA (severity)	• Fix based on severity • Triage & Assess	• Regular Review of vulnerability actions • Regular Burn down of Vulnerabilities by SLA	• Number of vulnerabilities • SLA per criticality
M3	• Policy mandating scanning requirements / Secure SDLC • Regular Pen-test / External Scan • Automated Static code analysis • Infra Vulnerability - L2 (Image Scanning, O/S - Servers, O/S - Endpoint, Installed Apps, Network Scanning) • Automated Library assessment / OSS-SCA • Code Peer review	• Aggregate vulnerabilities per business application • Aggregation of Assets • Asset contextualization (business) • Deduplication L1 - Automated - (Assets Dedup, CVE Dedup)	• Prioritization based on vulnerability severity • Prioritization based on Risk/ Risk Based SLA • Prioritization based on Cyber threat intelligence	• Fix based on Risk/ SLA • Triage & Assess / Exception management - L1 (False Positives)	• Regular review of Backlog • Regular Burn down of top vulnerabilities in the backlog	• SLA per criticality • SLA Risk based
M4	• Policy mandating scanning requirements / Secure SDLC • Bug Bounty/ Pentest • Automated Static analysis • Automated SCA • Automate TEST WEB/ DAST • API Assessment • Code Peer review • Infra Vulnerability - L3 (Image Scanning, O/S - Servers, O/S - Endpoint, Installed Apps, Network Scanning) • Container Scan • Cloud assessment/ IaC	• Aggregate vulnerabilities per business application • Aggregation of Assets • Asset contextualization (business) • Contextual Location of assets • Deduplication L2- Automated - (Assets Dedup, CVE Dedup, Contextual Deduplication) • Track the users / team operating on assets	• Prioritization based on vulnerability severity • Prioritization with Risk/ Risk based SLA • Prioritization based on Cyber threat intel • Prioritization based on business contextual information	• Fix based on Risk/ SLA • Triage & Assess / Triage & Schedule (sprint planning) - Backlog management • Exception management - L2 (Mitigation controls, False Positives)	• Regular review of Backlog • Regular Burn down of top vulnerabilities in the backlog • Reporting to Business line based on Risk level, • Feedback loop to dev on what to fix first. • Systemic Changes based on Security insights	• SLA per criticality • SLA Risk based • Mean time to resolution • Security balanceFalse Positive/ Exception rateSecurity insights
	• Policy mandating scanning	• Aggregate vulnerabilities Aggregation	• Prioritization based on vulnerability	• Fix based on Risk/ SLA	• Regular review of Backlog	• Mean time to resolution/MTTR

LEVEL	DETECTION / TESTING	AGGREGATION	PRIORITIZATION	VULNERABILITY ACTION	VULNERABILITY PROCESS	MEASUREMENT
DSOMM MAPPING	TEST & VERIFICATION	TRIAGE	TRIAGE	TRIAGE	CULTURE & ORG	MONITORING
SAMM V2 MAPPING	SECURITY TESTING	DEFECT MANAGEMENT	DEFECT MANAGEMENT	DEFECT MANAGEMENT	DEFECT MANAGEMENT	MEASURE & IMPROVE STREAM B
M1	• Policy mandating scanning requirements / Secure SDLC • Regular Pentest / External Scan • No SCA/ Library detection	• Aggregate Vulnerabilities in entral place	• Prioritization based on vulnerability severity	• Fix based on severity	• Reactive and Regular review of vulnerability actions	• Number of vulnerabilities/ Vulnerability Severity
M2	• Policy mandating scanning requirements / Secure SDLC • Regular Pen-test / External Scan • Ad-how Static analysis • Infra Vulnerability - L1 (O/S - Endpoint, Installed Apps) • SAST - Static Code Analysis or SCA	• Aggregate vulnerabilities per business application • Aggregation of Assets • Deduplication - L0 - Manual	• Prioritization based on vulnerability severity • Prioritization based on SLA (severity)	• Fix based on severity • Triage & Assess	• Regular Review of vulnerability actions • Regular Burn down of Vulnerabilities by SLA	• Number of vulnerabilities • SLA per criticality
M3	• Policy mandating scanning requirements / Secure SDLC • Regular Pen-test / External Scan • Automated Static code analysis • Infra Vulnerability - L2 (Image Scanning, O/S - Servers, O/S - Endpoint, Installed Apps, Network Scanning) • Automated Library assessment / OSS-SCA • Code Peer review	• Aggregate vulnerabilities per business application • Aggregation of Assets • Asset contextualization (business) • Deduplication L1 - Automated - (Assets Dedup, CVE Dedup)	• Prioritization based on vulnerability severity • Prioritization based on Risk/ Risk Based SLA • Prioritization based on Cyber threat intelligence	• Fix based on Risk/ SLA • Triage & Assess / Exception management - L1 (False Positives)	• Regular review of Backlog • Regular Burn down of top vulnerabilities in the backlog	• SLA per criticality • SLA Risk based
M4	• Policy mandating scanning requirements / Secure SDLC • Bug Bounty/ Pentest • Automated Static analysis • Automated SCA • Automate TEST WEB/ DAST • API Assessment • Code Peer review • Infra Vulnerability - L3 (Image Scanning, O/S - Servers, O/S - Endpoint, Installed Apps, Network Scanning) • Container Scan • Cloud assessment/ IaC	• Aggregate vulnerabilities per business application • Aggregation of Assets • Asset contextualization (business) • Contextual Location of assets • Deduplication L2- Automated - (Assets Dedup, CVE Dedup, Contextual Deduplication) • Track the users / team operating on assets	• Prioritization based on vulnerability severity • Prioritization with Risk/ Risk based SLA • Prioritization based on Cyber threat intel • Prioritization based on business contextual information	• Fix based on Risk/ SLA • Triage & Assess / Triage & Schedule (sprint planning) - Backlog management • Exception management - L2 (Mitigation controls, False Positives)	• Regular review of Backlog • Regular Burn down of top vulnerabilities in the backlog • Reporting to Business line based on Risk level, • Feedback loop to dev on what to fix first. • Systemic Changes based on Security insights	• SLA per criticality • SLA Risk based • Mean time to resolution • Security balanceFalse Positive/ Exception rateSecurity insights
M5	• Policy mandating scanning requirements / Secure SDLC • Automated Pentest • Bug Bounty/Pentest • Automated Static Analysis Automated SCA • Automated DAST WEB/ Automated API • Container Scan / Preflight Container Build • Code Peer review • Infra Vulnerability - L3 (Image Scanning, O/S - Servers, O/S - Endpoint, Installed Apps, Network Scanning) • Cloud assessment/ Automated IaC	• Aggregate vulnerabilities Aggregation of Assets Deduplication L3 - (Assets Dedup, CVE Dedup, Automated Function SCA-SAST, Contextual Deduplication) • Self Declared Asset/ Centralization of assets declaration • Contextualization (business) with Business Impact • Self Declared Contextual Location of assets/ Tag based • Track the users / team operating on assets • Track new assets automatically	• Prioritization based on vulnerability severity • Prioritization with RISK/ Risk based SLA, • Prioritization based on TEAM OKR • Prioritization based on Cyber threat intel, • Prioritization based on Contextual information • Prioritization based on business contextual information,	• Fix based on Risk/ SLA • Triage & Assess / Triage & Schedule (sprint planning) - Backlog management • Exception management - L3 (Mitigation controls, False Positives, Risk Acceptance)	• Regular review of Backlog • Regular Burn down of top vulnerabilities in the backlog Reporting to Business line based on Risk level, • Burn-down rate • Insights and strategic action based on the vulnerability observed Feedback loop to dev on what to fix first.Systemic Changes based on Security insights	• Mean time to resolution/MTTR • Users Stories vs Security • Security backlog burndown • SLA Risk based ,False Positive/ Exception rate • Technology Insights • Security OKR • Security Insights • Build vs Fix stories • Localized insights (per business application)

Metrics at different levels

Reporting



KPI

- **Scorecards**
- **Risk Level**
- Fix time/ Build time
- Regulation impact
- Financial Impact

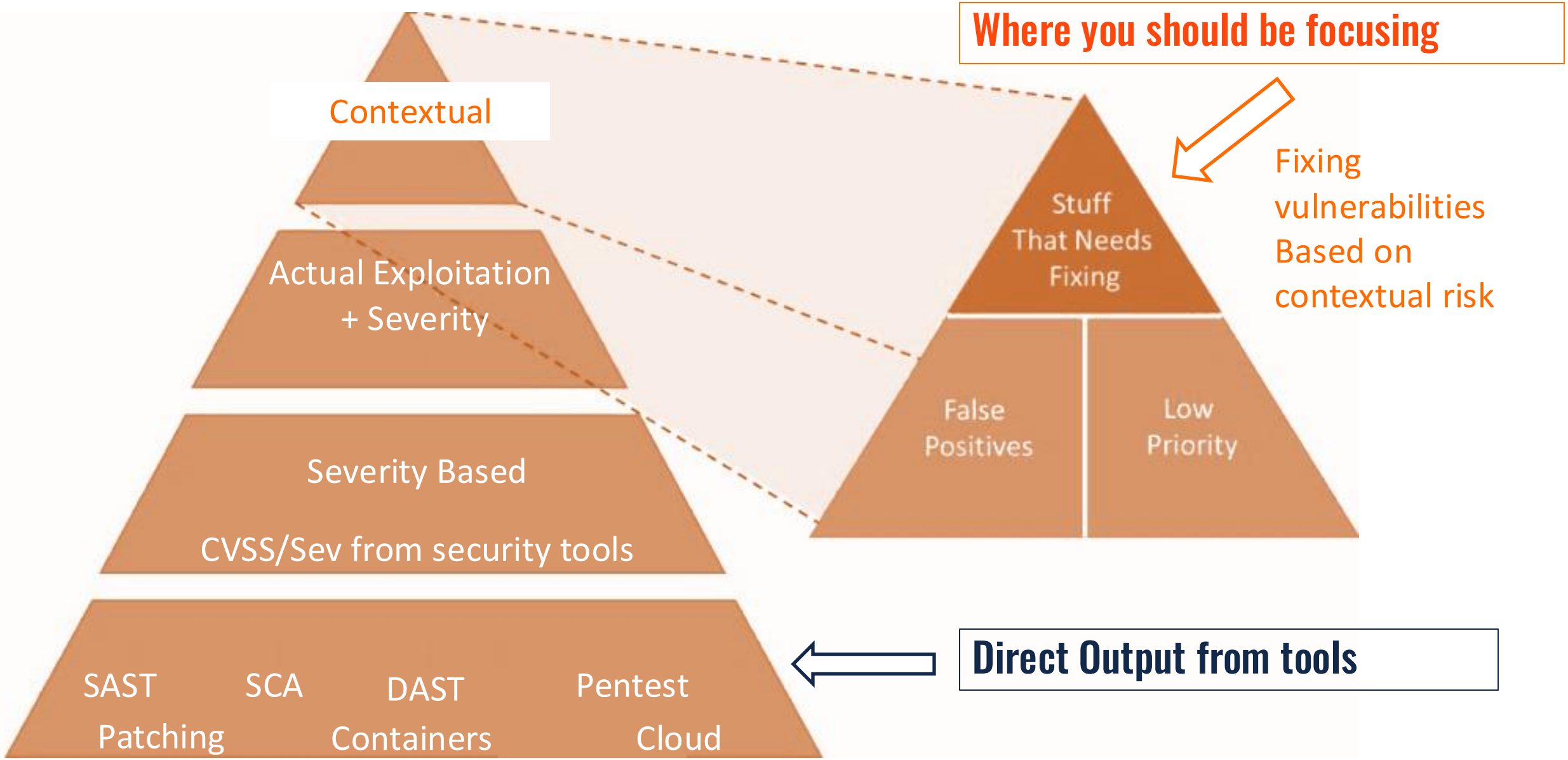
KPI

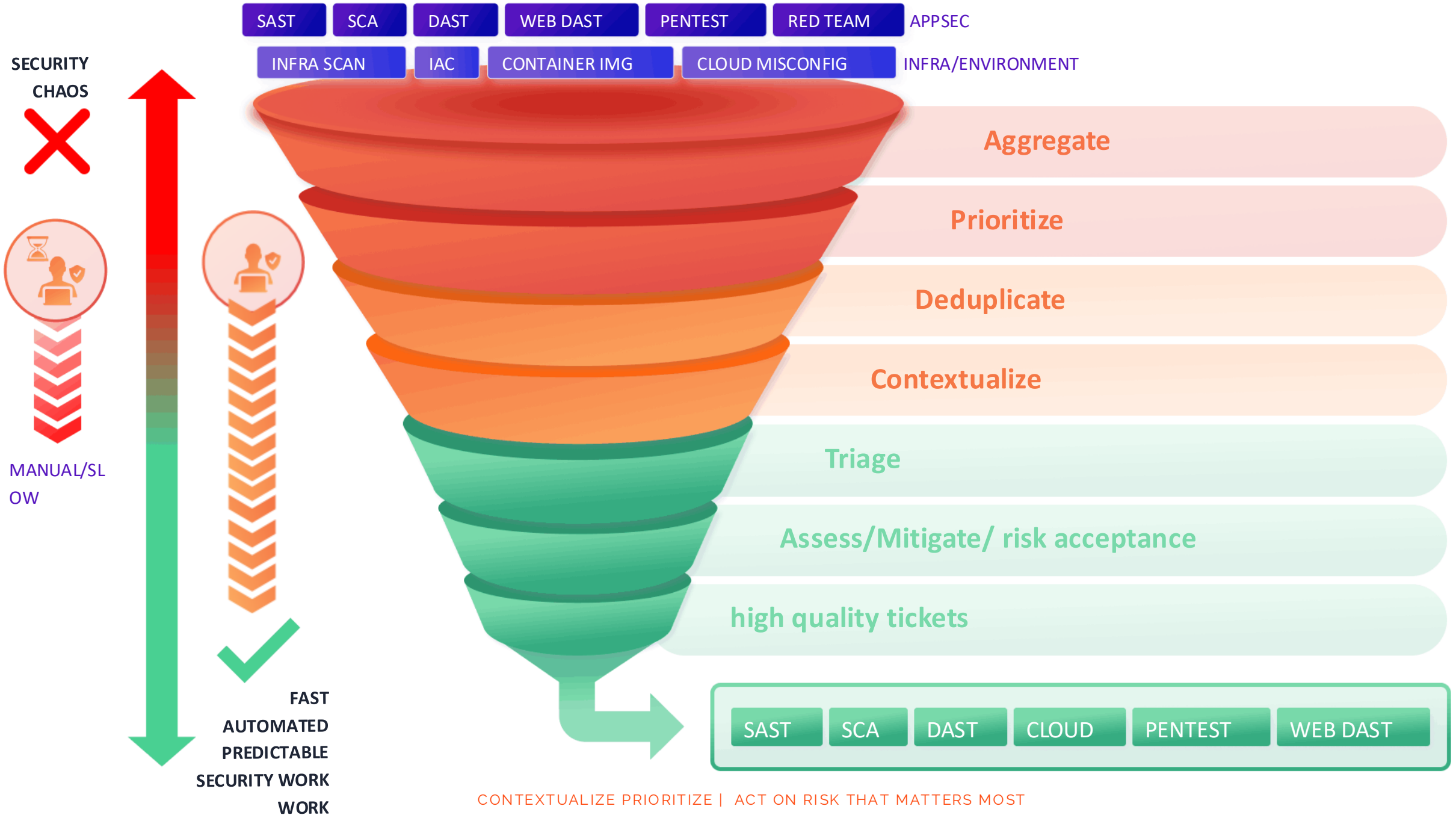
- Application/ Service **Risk**
- Trendline, Fixing vs building
- Critical alerts, SLA breach

KPI

- Vulnerability trending by categories
- Vulnerability categories trending
- Ticket open/Closed (MTTR, MTTO)
- Most critical vulnerability, assets

Prioritization is so 90....





CONTEXTUALIZE PRIORITIZE | ACT ON RISK THAT MATTERS MOST

PHOENIX SECURITY

ACT ON CONTAINER VULN

ACT ON ENDPOINT VULN

ACT ON CLOUD VULN

CONTEXTUALIZE, PRIORITIZE & ACT ON RISK

ACT ON APPSEC VULN

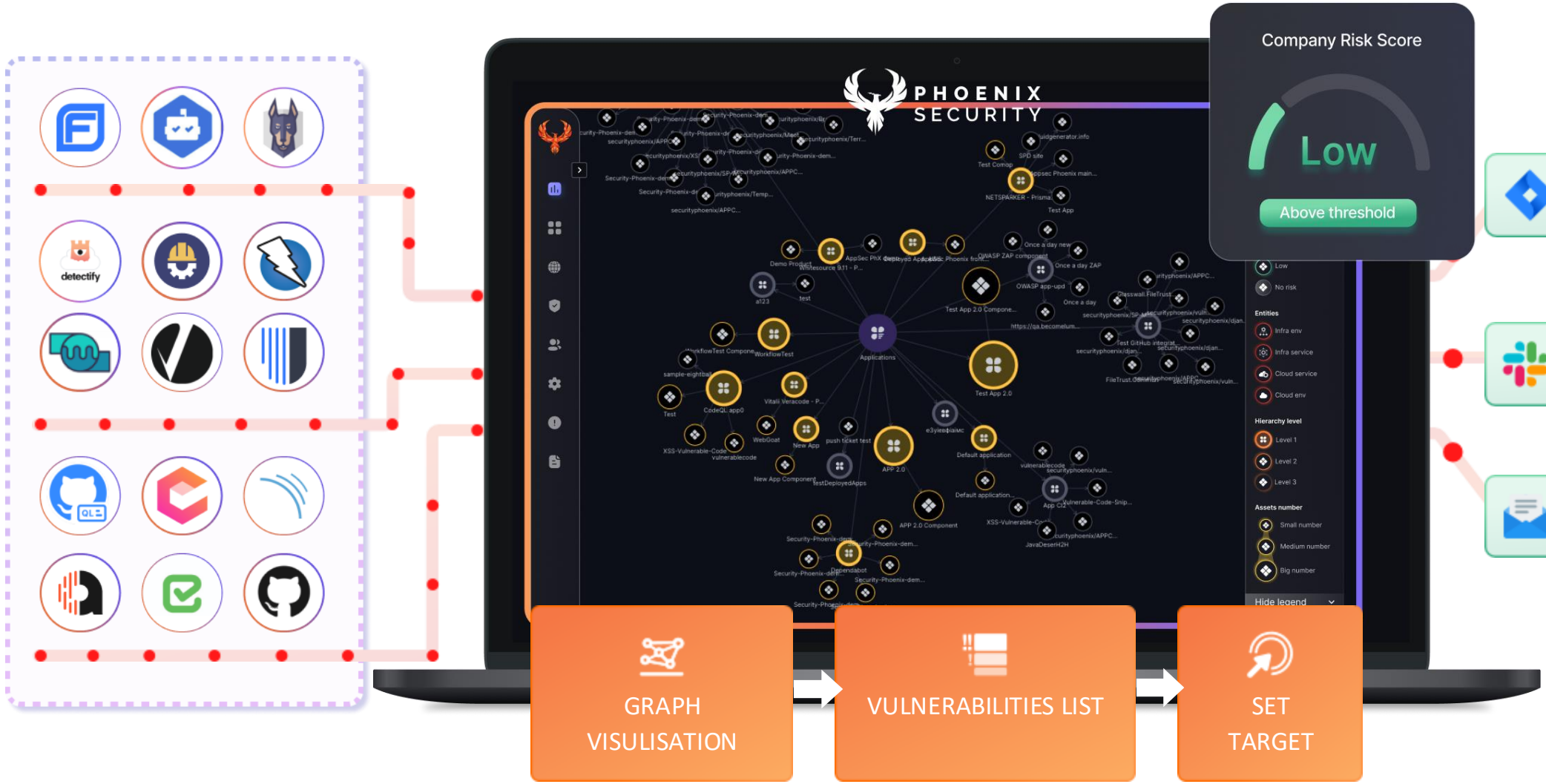
ACT ON INFRA VULN

ACT ON CODE VULN

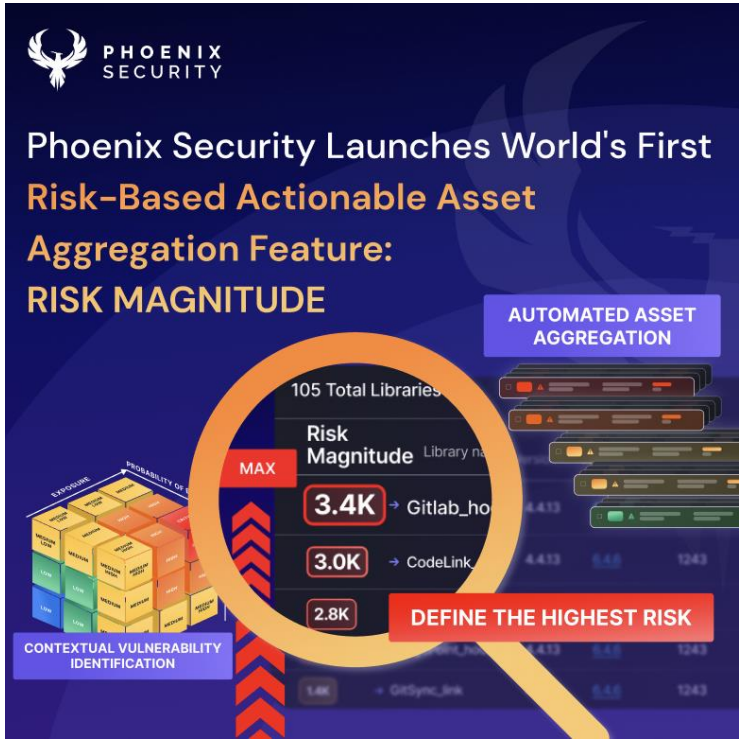
ACT ON SBOM VULN

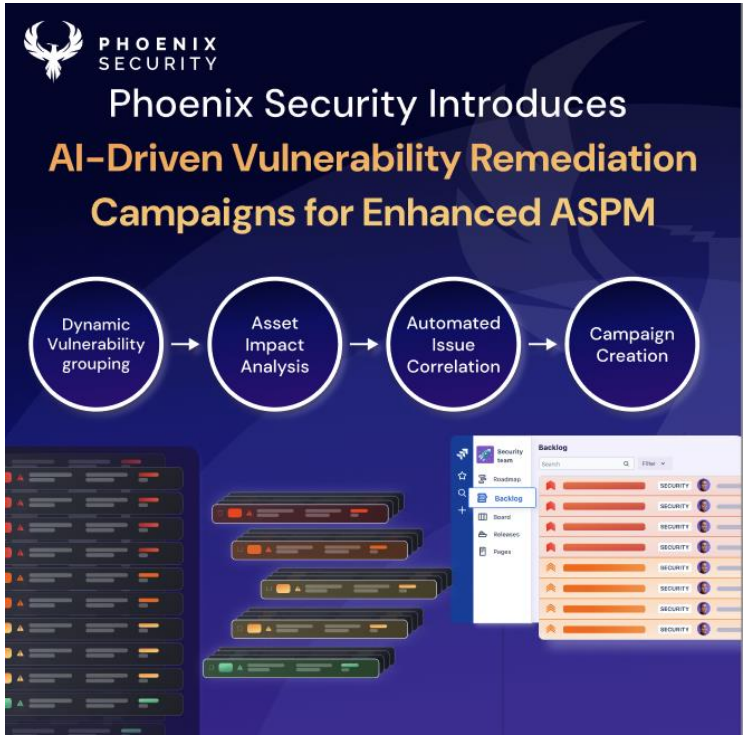
Phoenix Security Unify ASPM & CSPM for a contextual approach

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

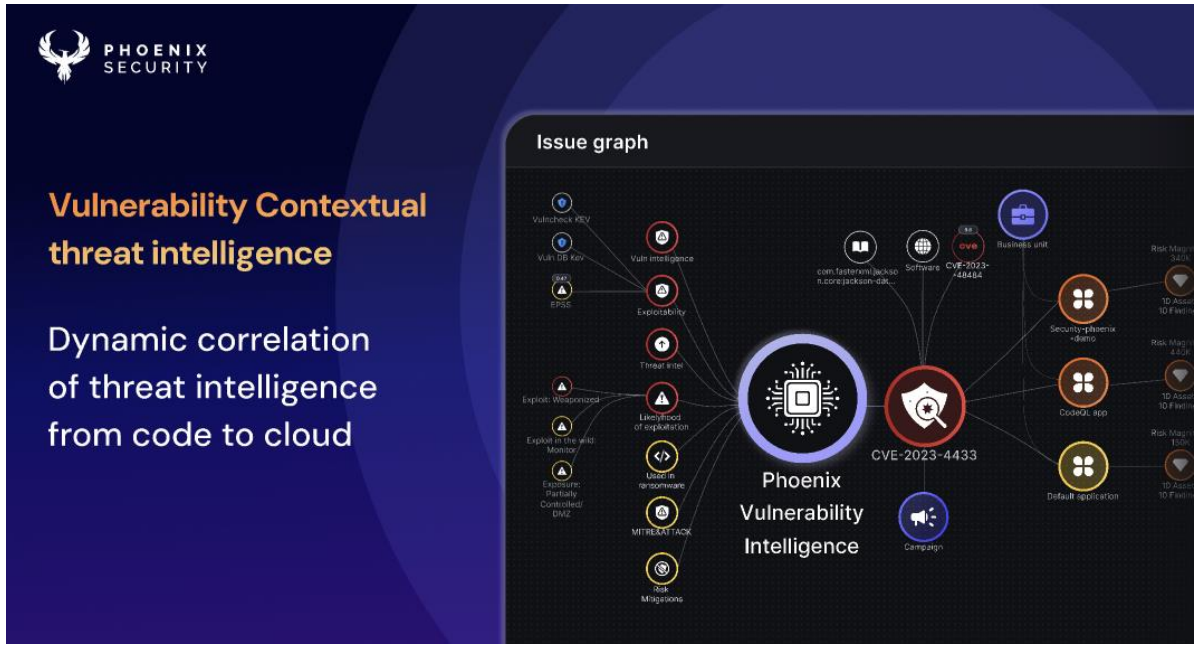


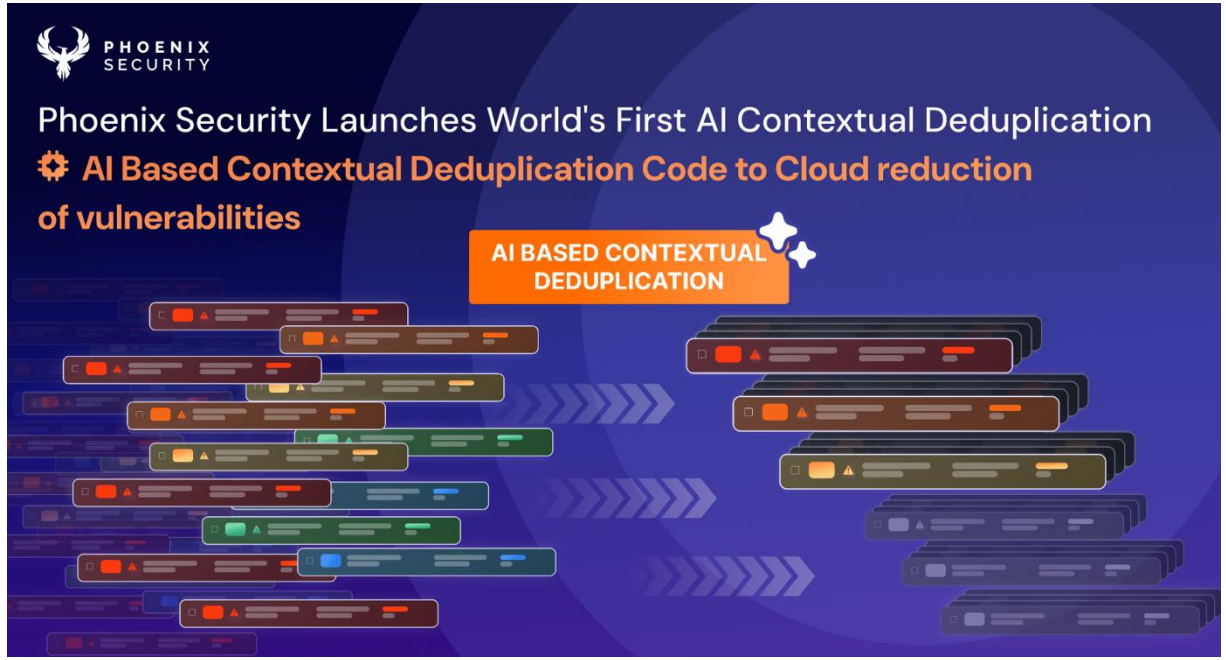
New Features





Upcoming New Features

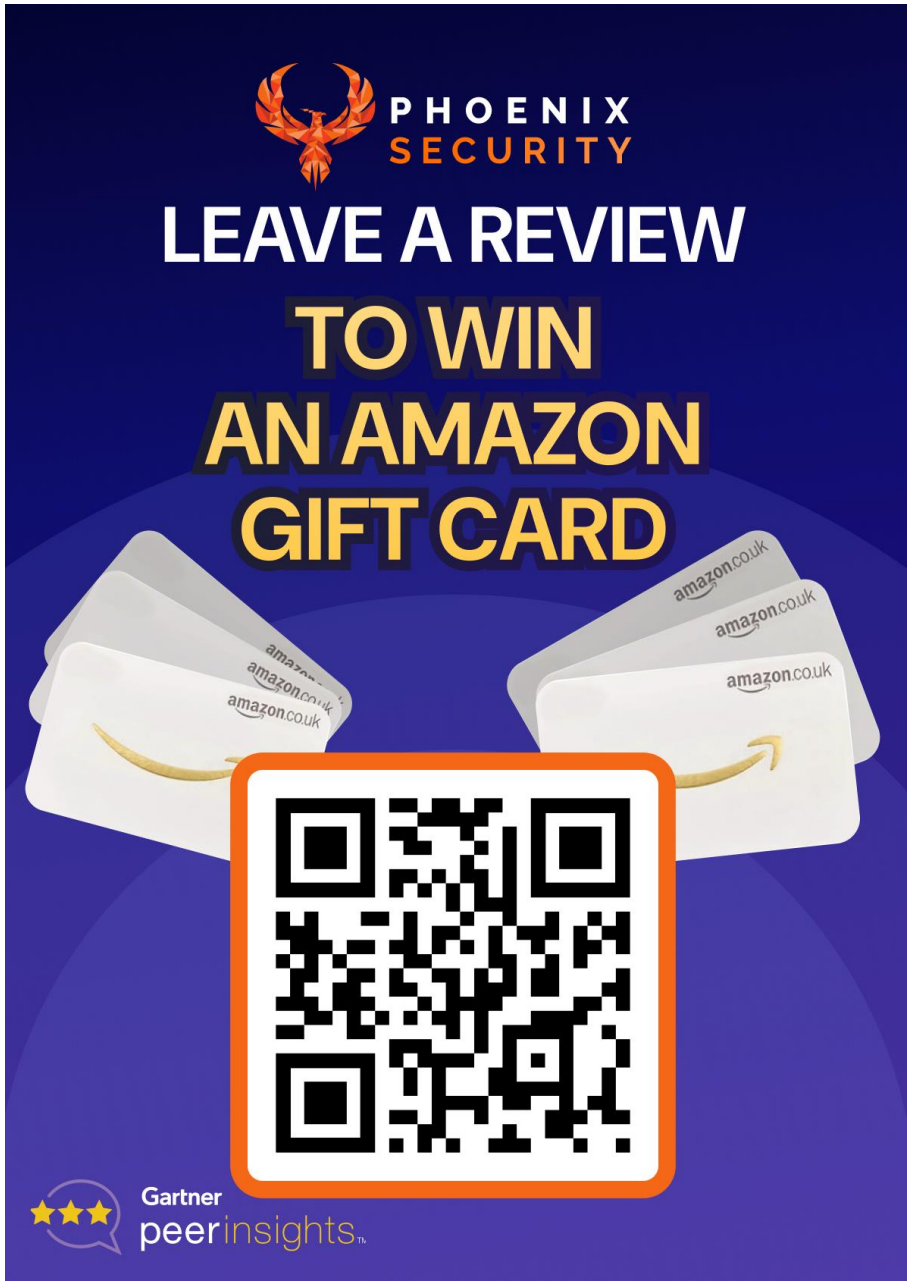




Partnership

Threat Intelligence

Cloud Integrations



Building resilient application and cloud security programs

OWASP 2024 GLOBAL AppSec

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

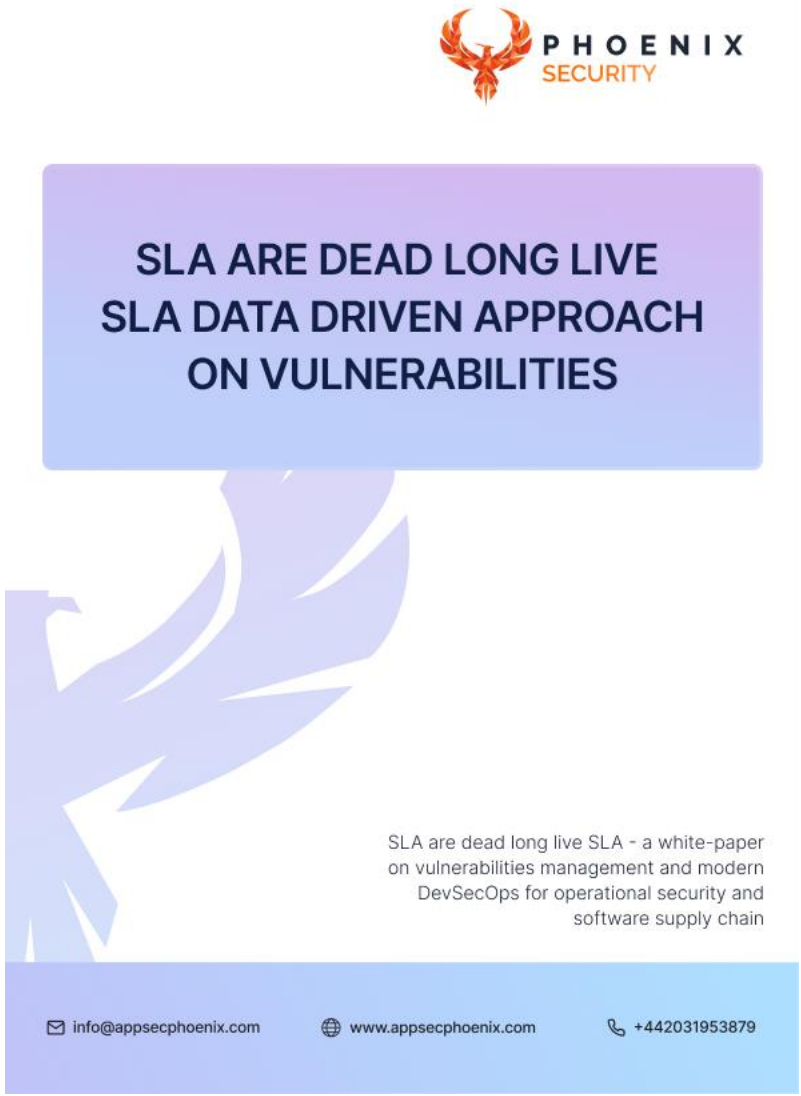
ACT ON APPSEC VULN

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

OWASP 2024 GLOBAL AppSec

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 pricritization

- 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 doud 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 doud-cloud and correlate threat inel

Removing Manual work to automate, scale effectively security teams

$ 1.780 K PROGRAM COST	1800 DAYS	»	226.6 K PROGRAM COST	150 DAYS

	Without AppSec Phoenix		APPSEC PHOENIX 7X CHEAPER 12X FASTER	
DESCRIPTION	COST	TIME	COST	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

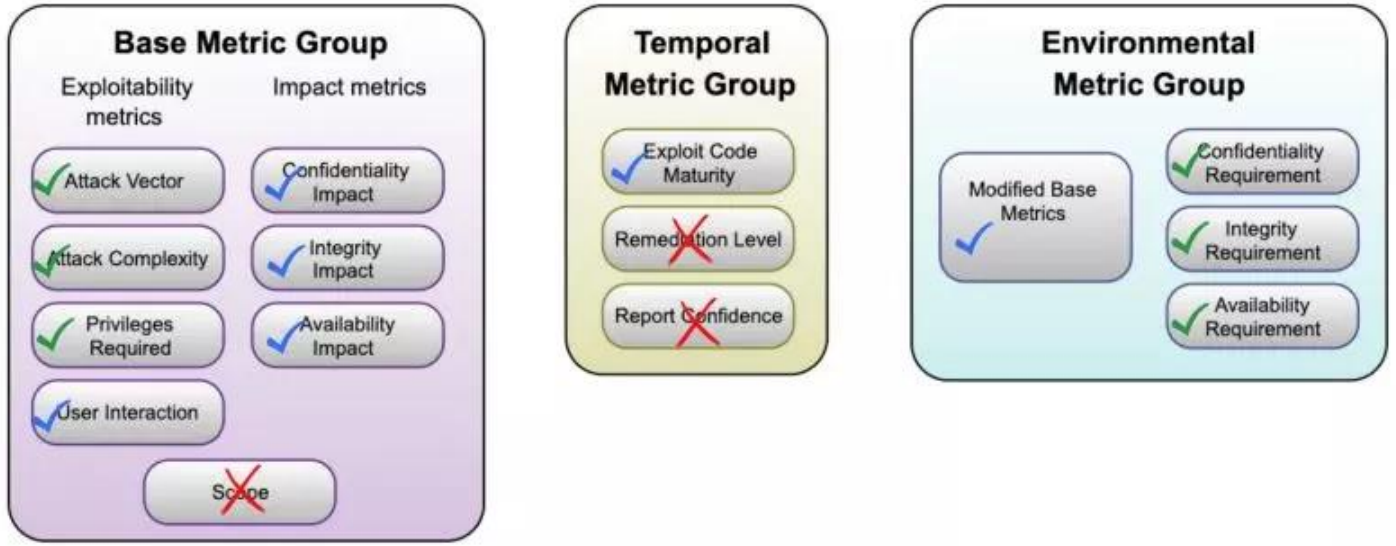
*DevSecOps average daily rate 500$,
Dev average daily rate 300$

Market Landscape

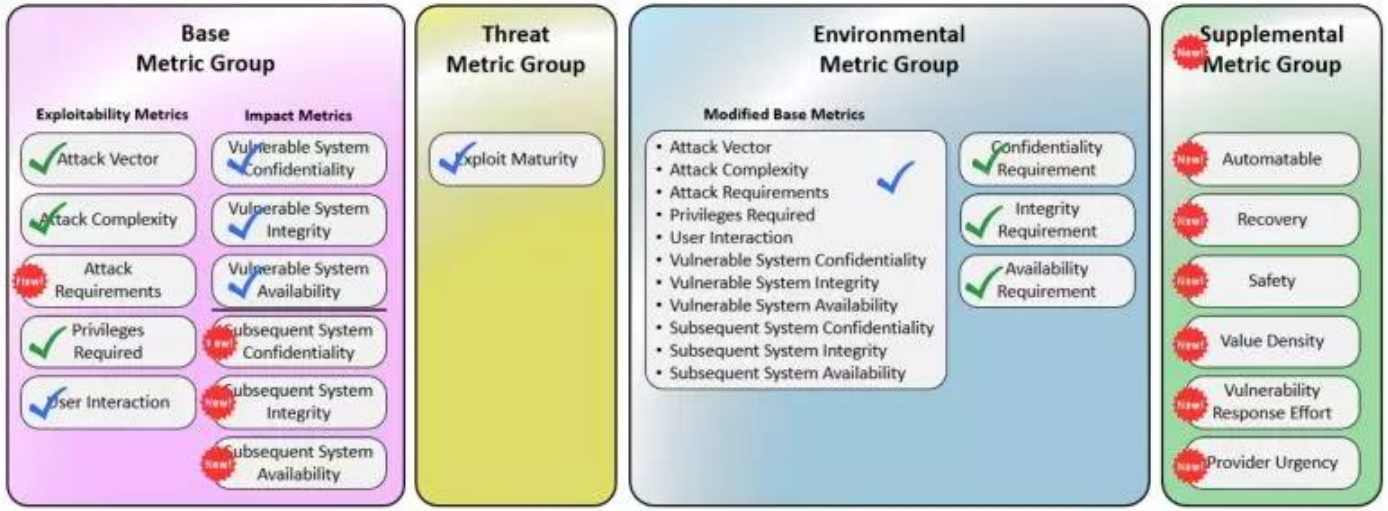
CVSS V40 vs 3.1

CVSS SCORE	ONE PER VULNERABILITY	MULTIPLE PER VULNERABILITY
BASE METRICS	EPLOITABILITY METRICS 4	EPLOITABILITY (5) - ATTACK REQUIREMENTS MORE GRANULAR
	IMPACT METRICS	WIDER ATTACK METRIC
	USER INTERACTION (2)	USER INTERACTION (3) INTRODUCTION OF PASSIVE
OTHER METRICS	ENVIRONMENTAL, TEMPORAL	ENVIRONMENTAL, TEMPORAL, MORE CUSTOMISATION
THREAT METRIC	TEMPORAL (3)	THREAT - NEW EPXLOIT MATURITY METRIC
ENVIRONMENTAL METRICS	ENVIRONMENTAL GROUP	MODIFIED CASE METRICS (11)
	ENVIRONMENTAL METRICS (8)	ENVIRONMENTAL METRICS (8)
CHAIN OF ATTACKS	N/A	SUBSEQUENT SYSTEM
LOCALITY/LOCATION CONTEXT	N/A	N/A
BUSINESS CRITICALITY	BASIC - CIA (3)	BASIC - CIA (3)
CUSTOMISATION	LIMITED	ADVANCED

Common Vulnerability Scoring System v3.1



Common Vulnerability Scoring System v4

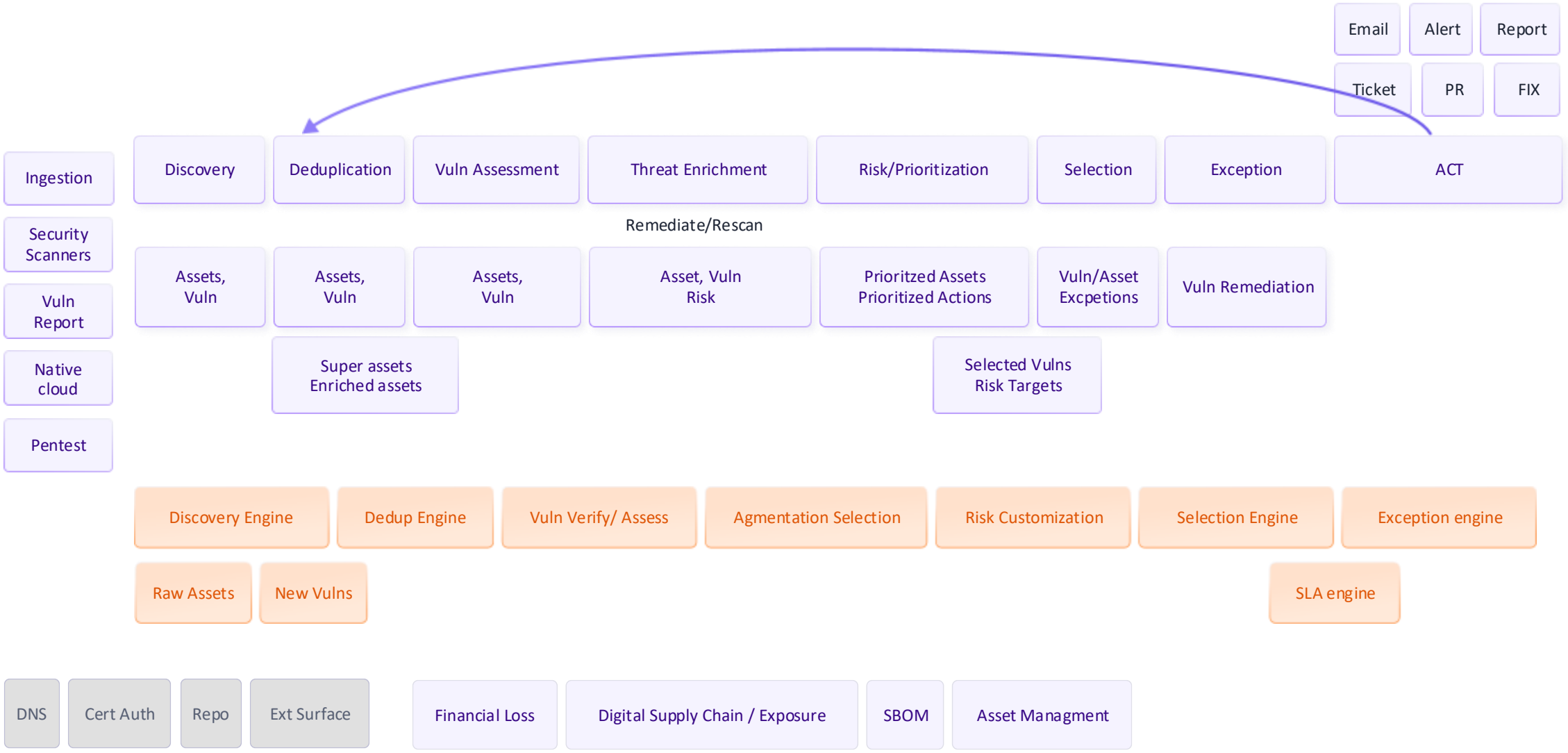


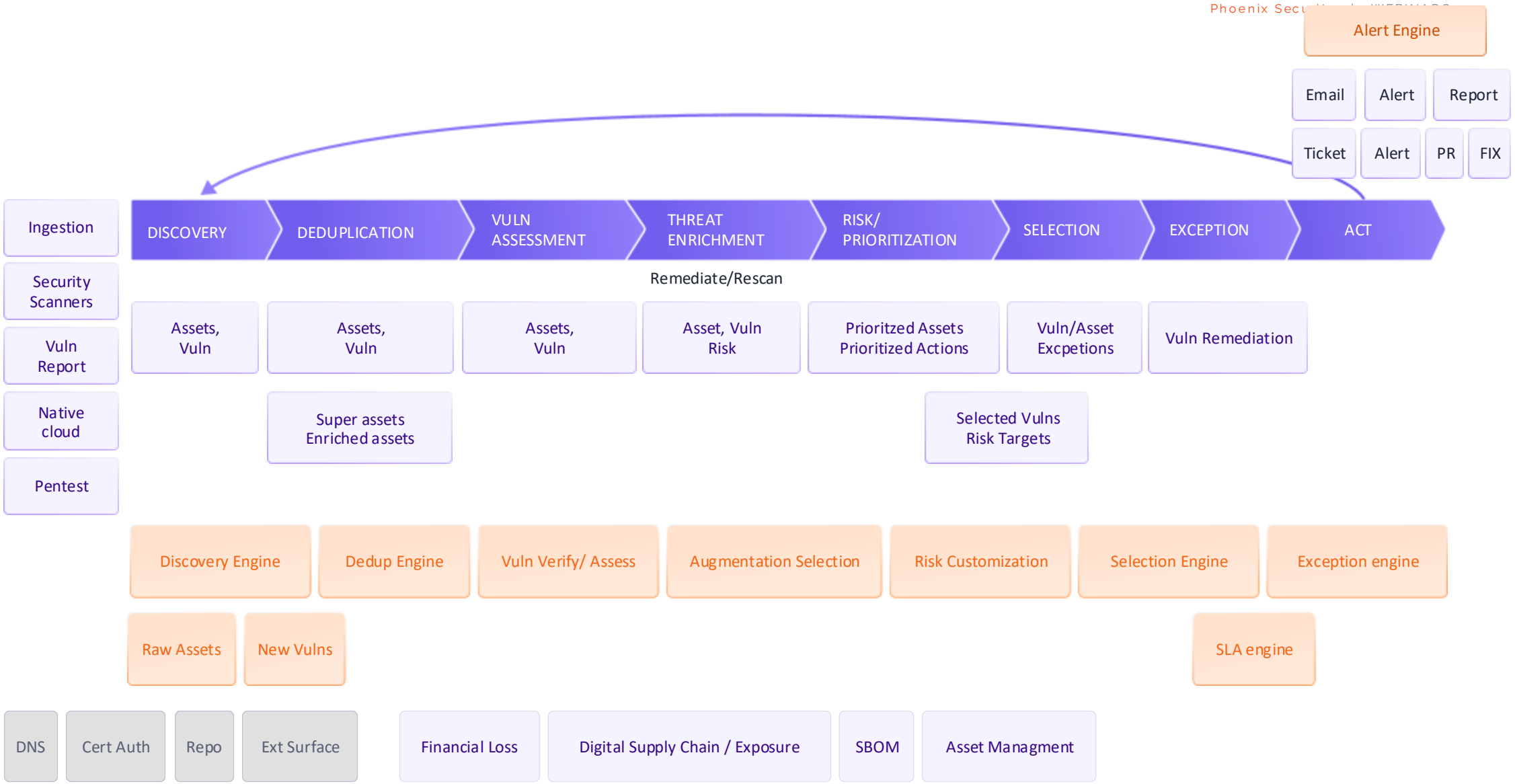
Credit Patrick Gerrit

Phoenix security unifies risk across all your attack surface, prioritize vulnerabilities from code to cloud

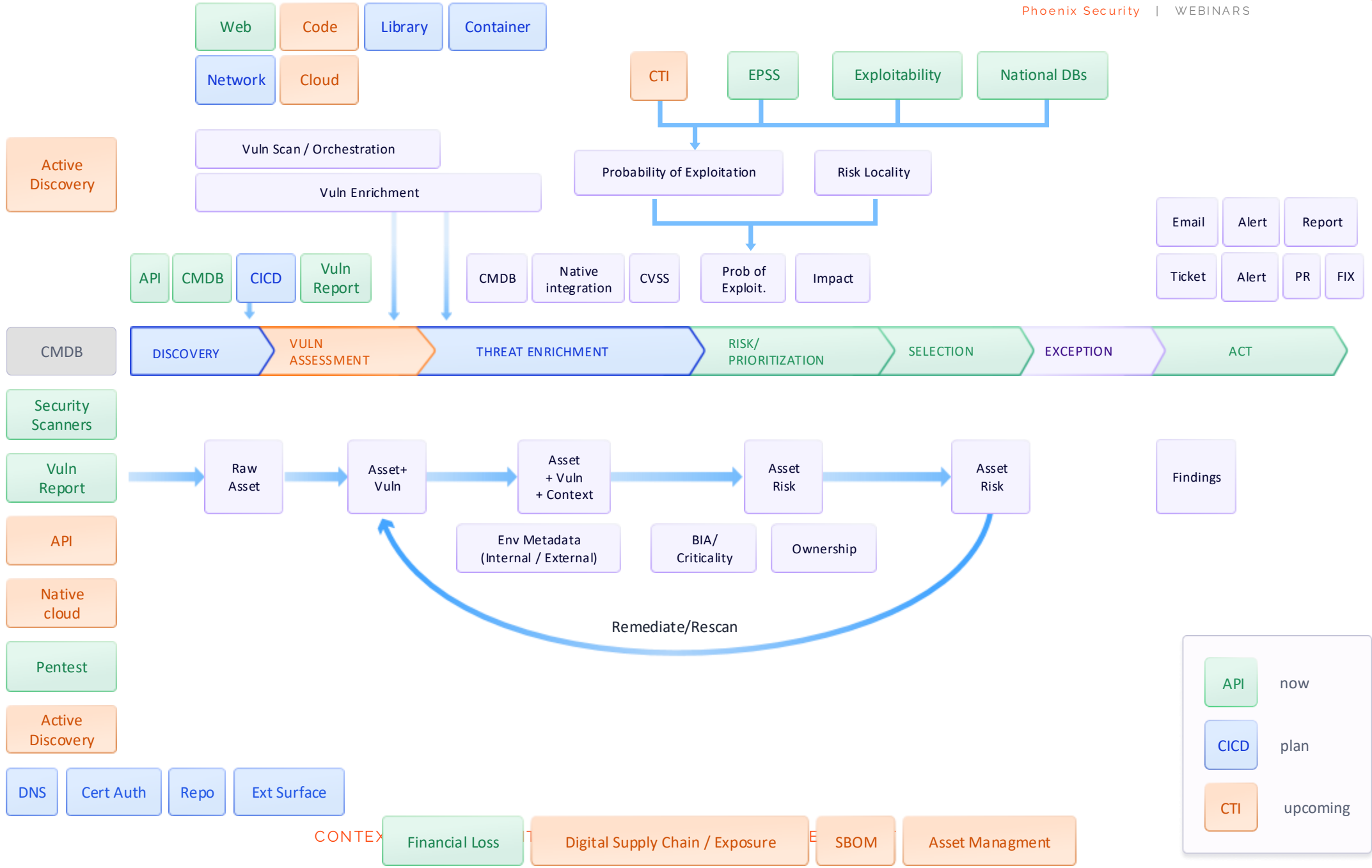
Appendix

Full asset Lifecycle 1.5 – Moving into Engines with Customization from users

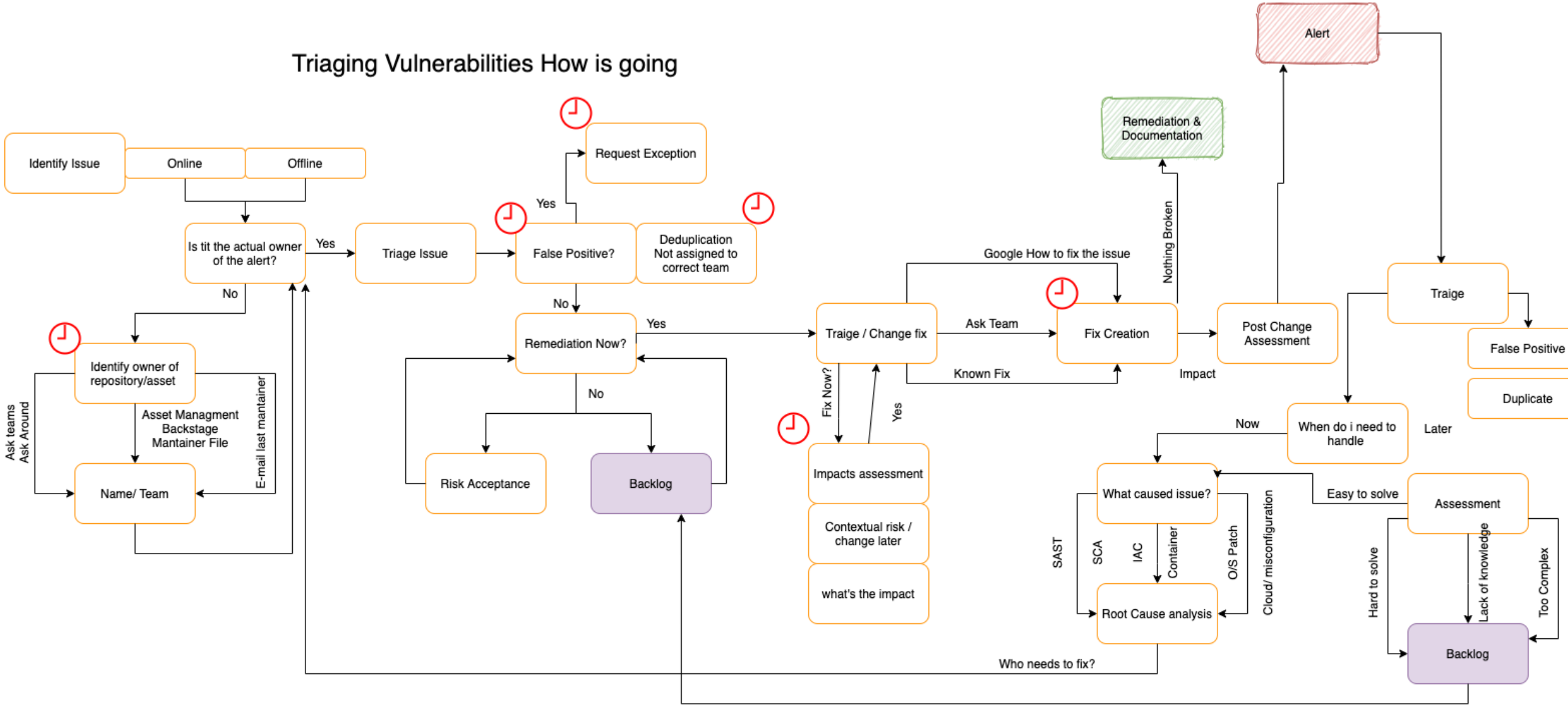



Alert Engine
Email
Alert
Report
Ticket
Alert
PR
FIX
Ingestion
Security Scanners
Vuln Report
Native cloud
Pentest
DISCOVERY
DEDUPLICATION
VULN ASSESSMENT
THREAT ENRICHMENT
RISK/ PRIORITIZATION
SELECTION
EXCEPTION
ACT
Remediate/Rescan
Assets, Vuln
Assets, Vuln
Assets, Vuln
Asset, Vuln Risk
Prioritzed Assets Prioritized Actions
Vuln/Asset Excpetions
Vuln Remediation
Super assets Enriched assets
Selected Vulns Risk Targets
Discovery Engine
Dedup Engine
Vuln Verify/ Assess
Augmentation Selection
Risk Customization
Selection Engine
Exception engine
Raw Assets
New Vulns
SLA engine
DNS
Cert Auth
Repo
Ext Surface
Financial Loss
Digital Supply Chain / Exposure
SBOM
Asset Managment

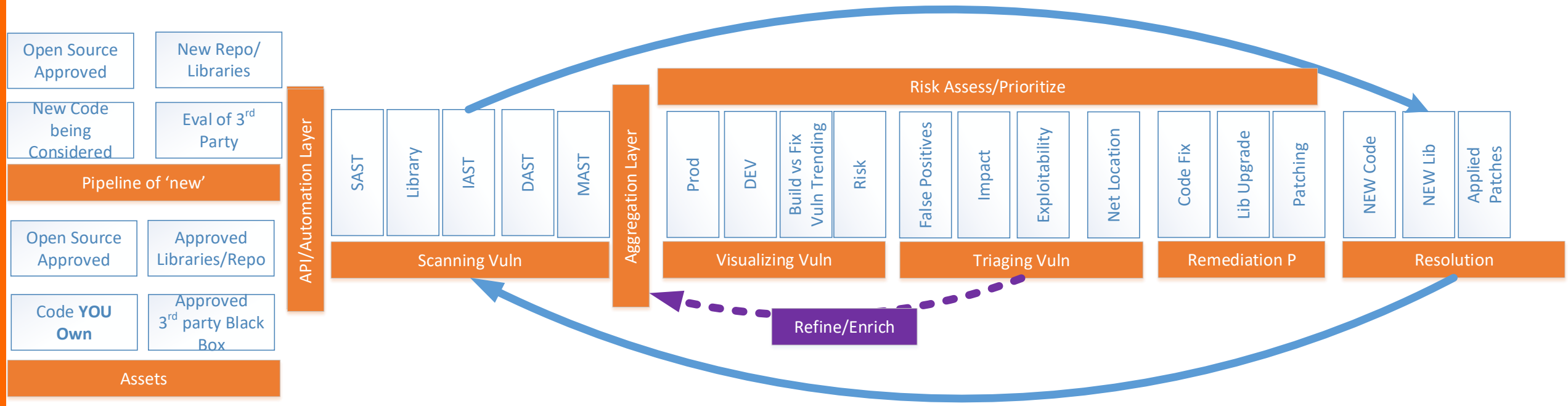
Roadmap of development from now to full asset lifecycle



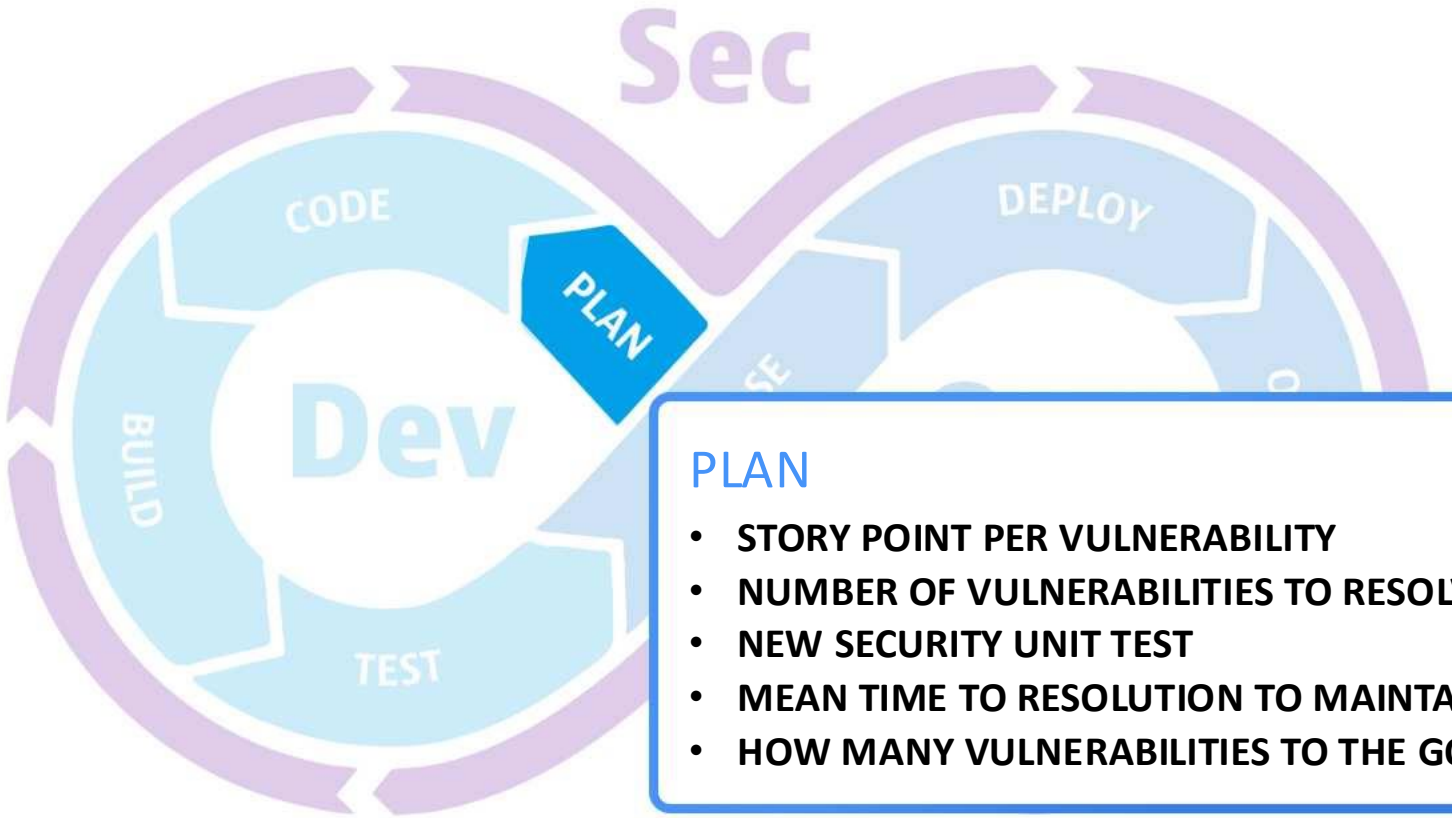
Triage is complex



Triage – Linear ?



SDLC Flow Stage

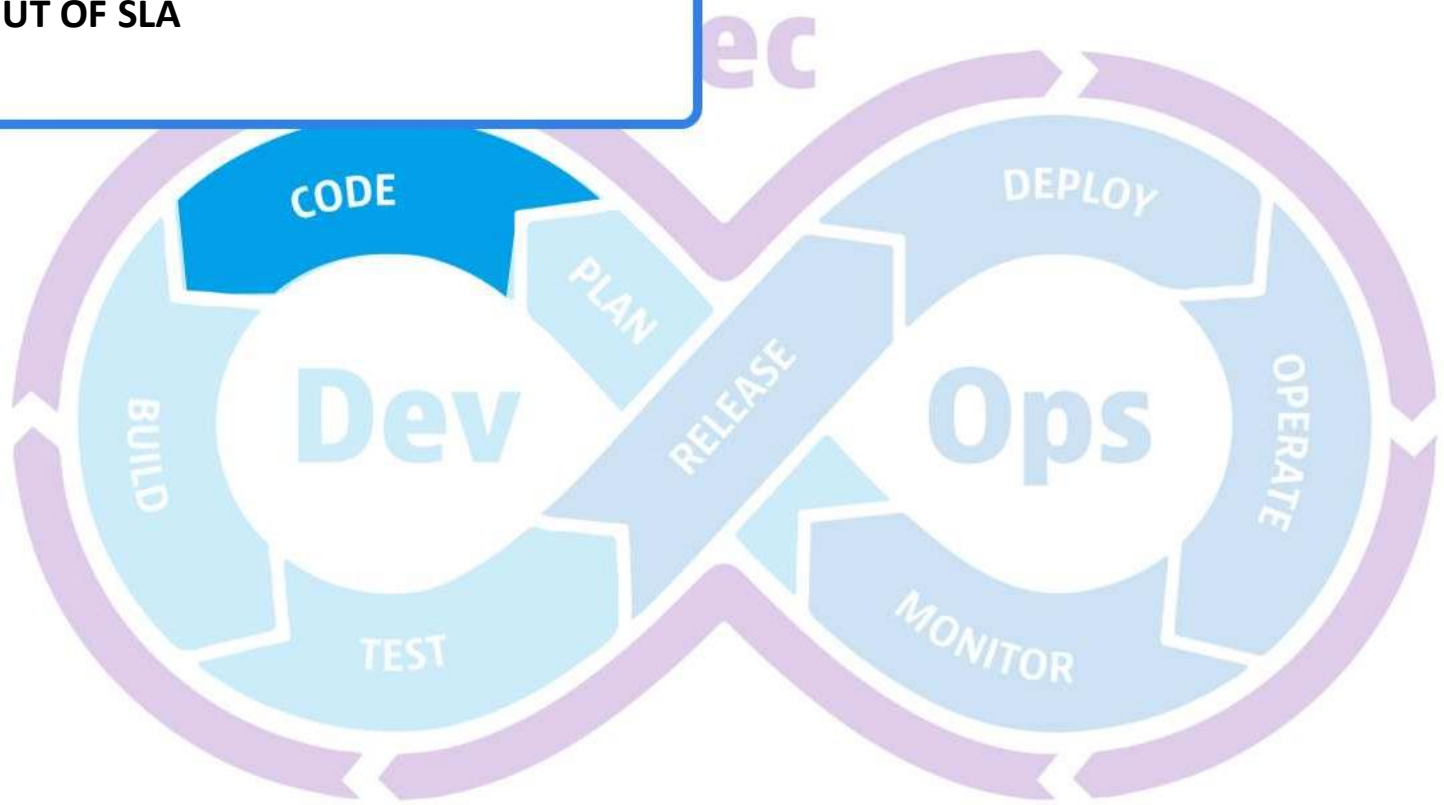


PLAN

- **STORY POINT PER VULNERABILITY**
- **NUMBER OF VULNERABILITIES TO RESOLVE**
- **NEW SECURITY UNIT TEST**
- **MEAN TIME TO RESOLUTION TO MAINTAIN**
- **HOW MANY VULNERABILITIES TO THE GOAL**

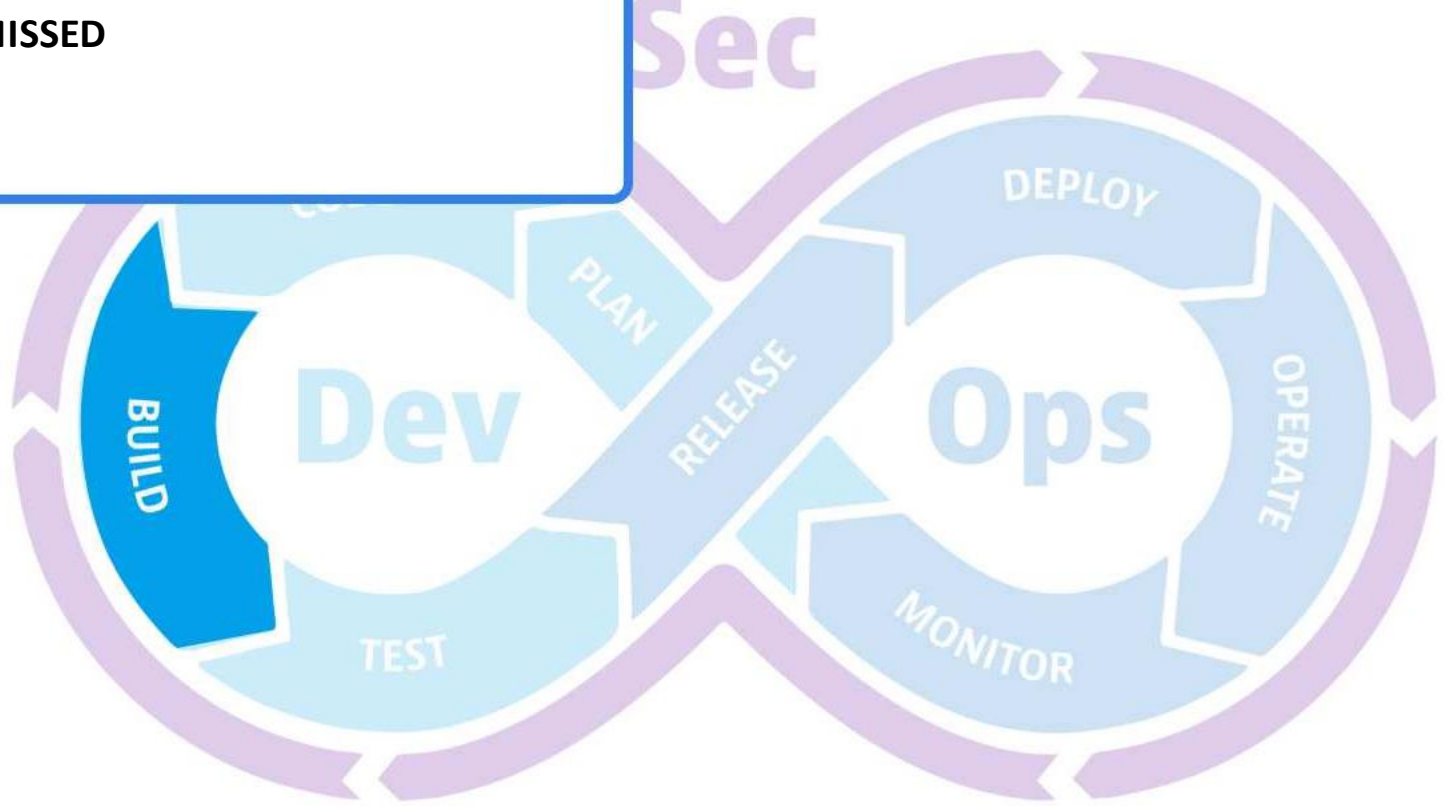
CODE

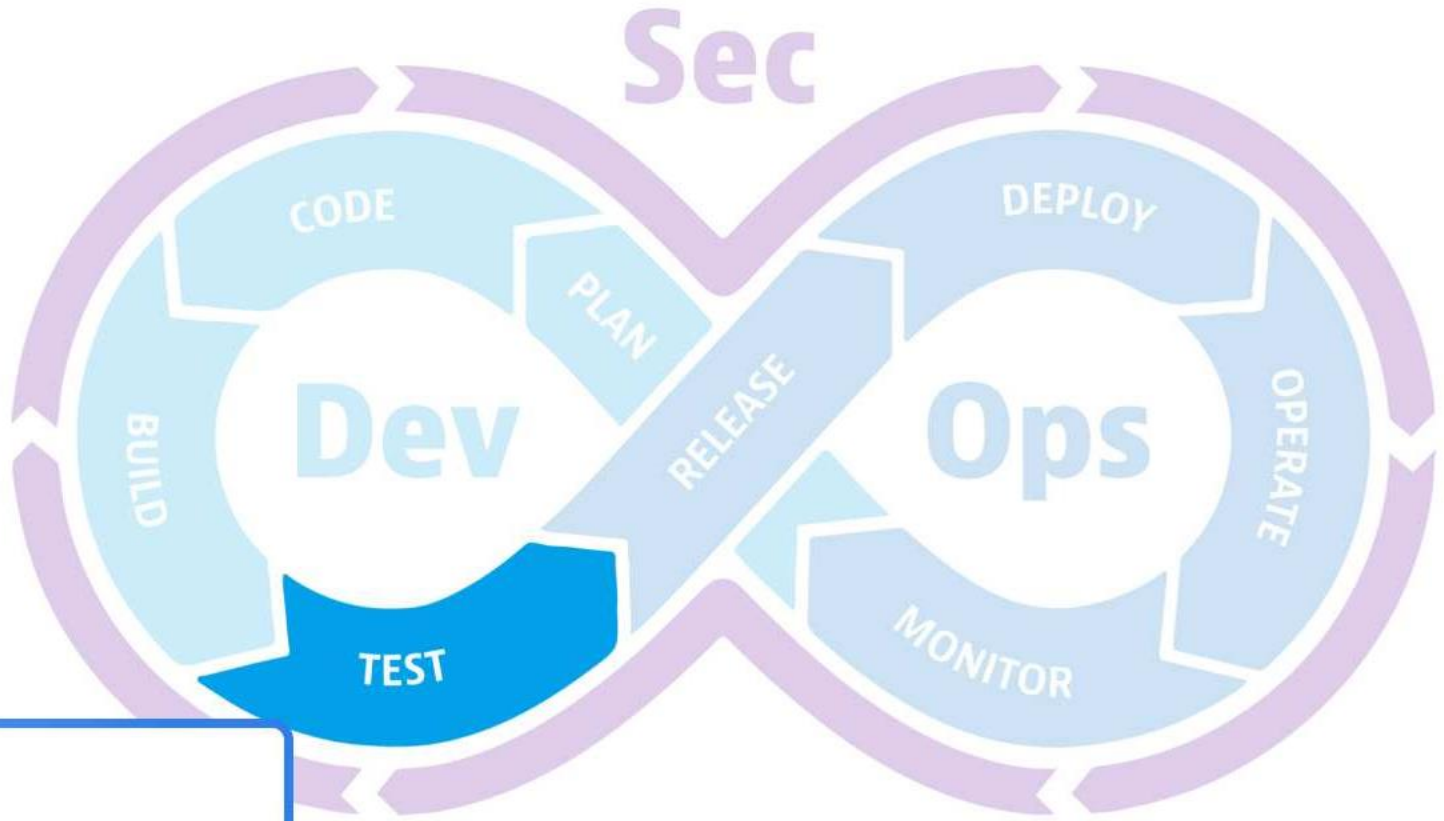
- **SCANNING CODE WITH ISSUE IN IDE**
- **COMMON ISSUE ACROSS MULTIPLE CODE BASES**
- **HIGH/MEDIUM RISK ELEMENTS**
- **VULNERABILITIES IN / OUT OF SLA**
- **SECURITY STORIES**



BUILD

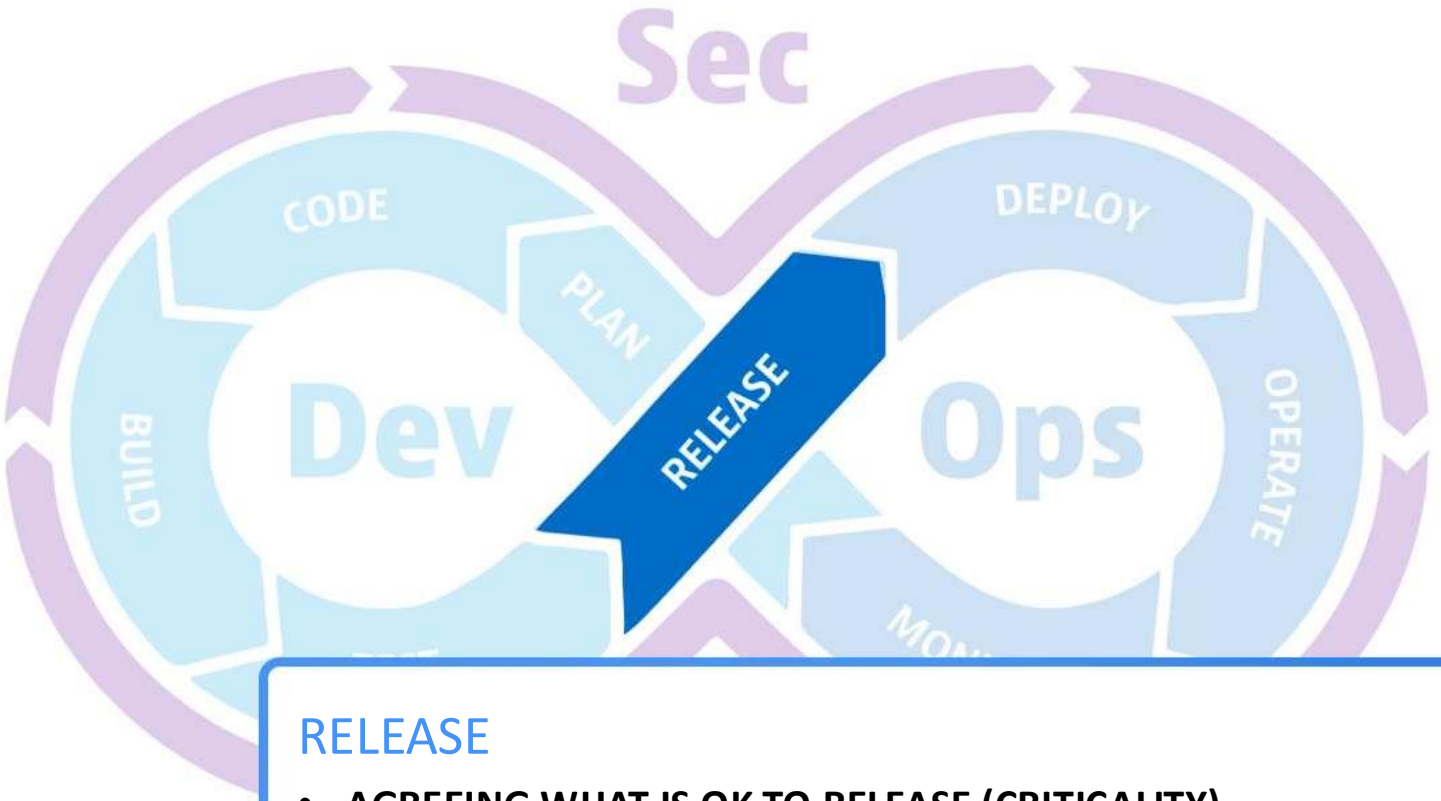
- **IAST/DAST FOR CODE BUILT**
- **LIBRARIES AND DEPENDENCY VULNERABILITIES**
- **SECURITY STORIES HIT/MISSED**
- **RISK ITEMS (TOP/LOW)**
- **ITEMS IN/OUT SLA**





TEST

- **DAST OUTPUT/ IAST OUTPUT**
- **SECURITY TESTING/ FIXES**
- **BACKLOG OF SECURITY ITEMS**

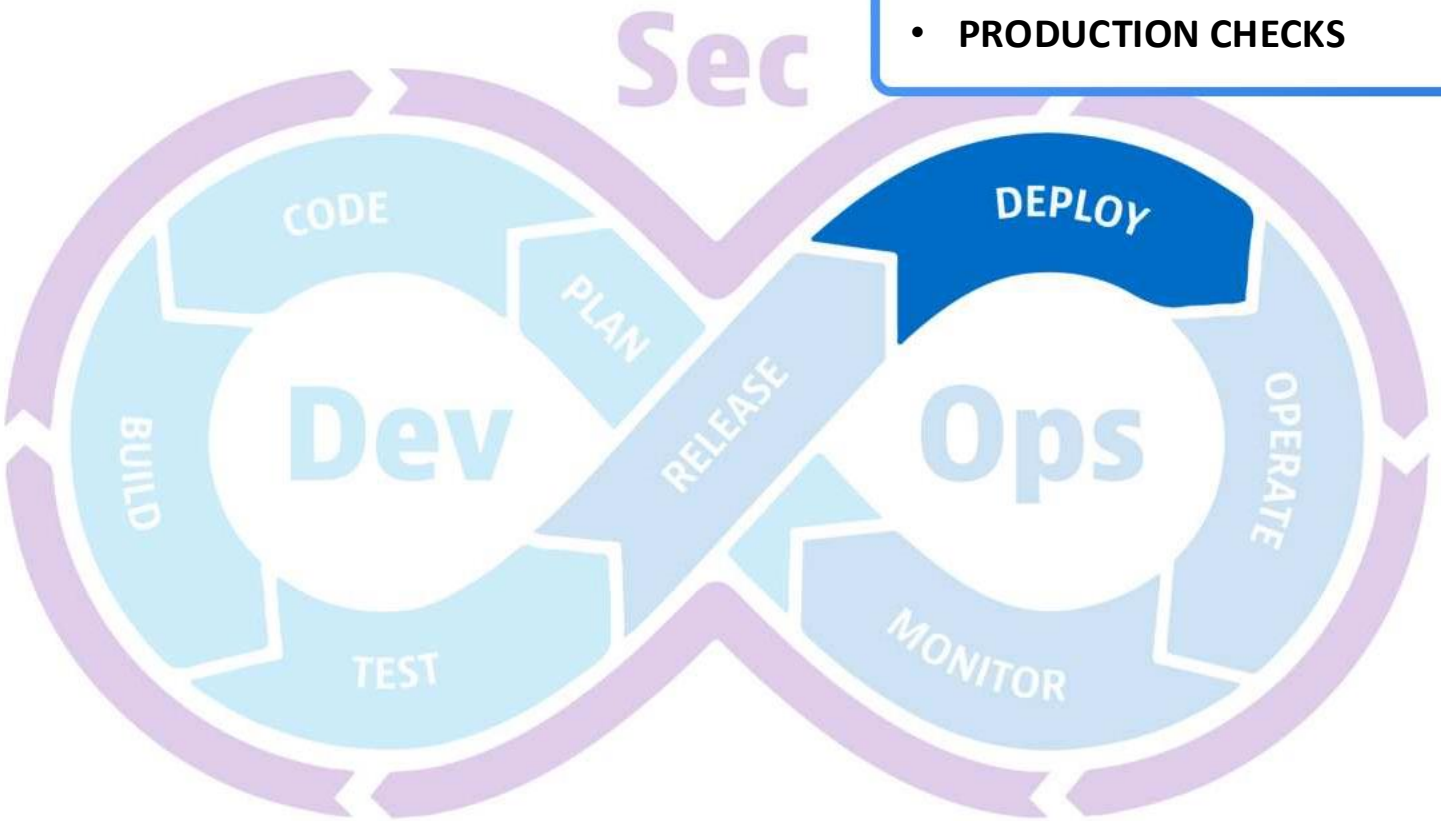


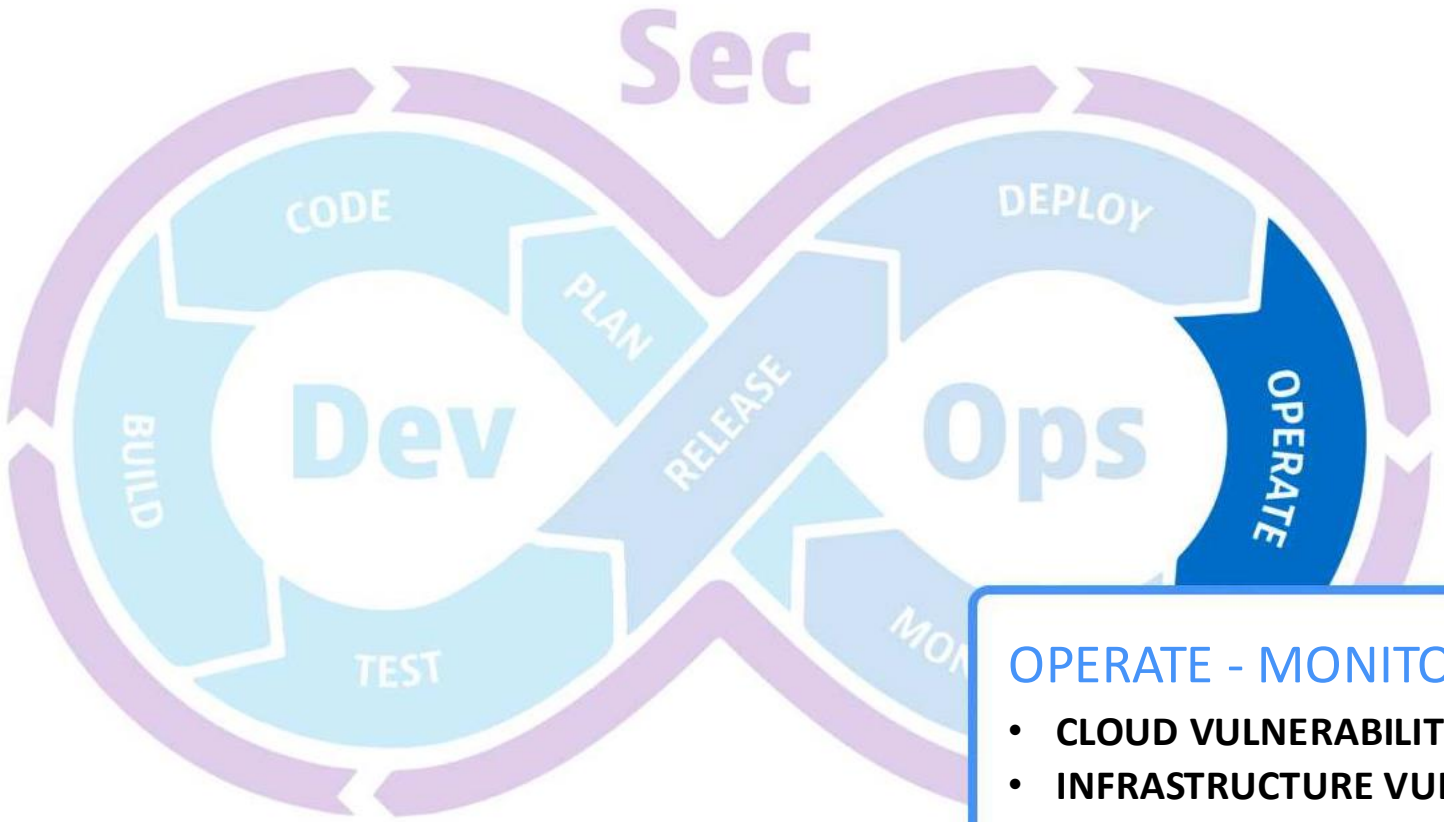
RELEASE

- **AGREEING WHAT IS OK TO RELEASE (CRITICALITY)**
- **BREAK POINT - RELEASE OR NOT WITH VULNERABILITIES**
- **MEAN TIME TO RESOLUTION DECISION**
- **LICENCE TO DEPLOY**

DEPLOY

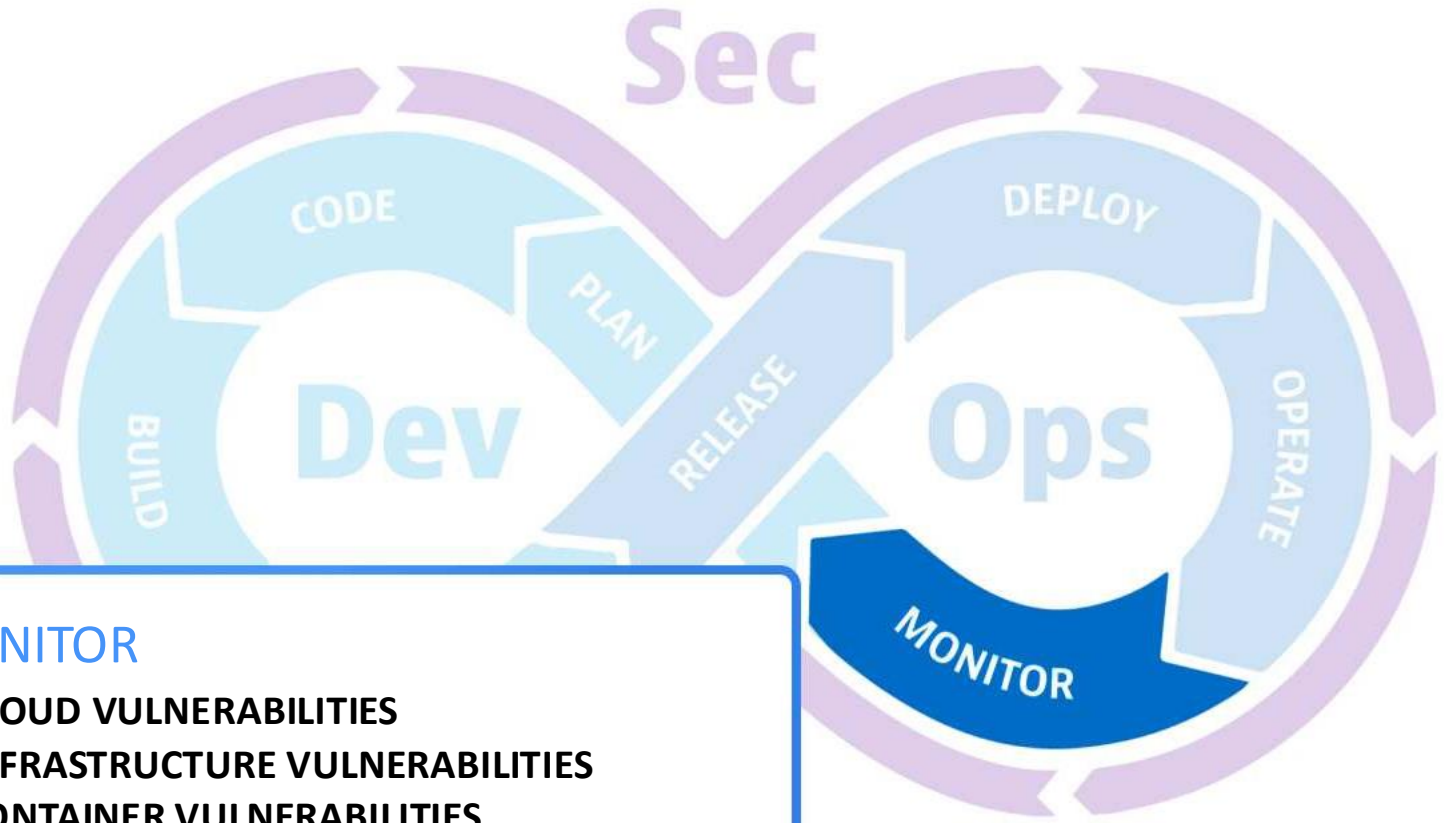
- **BREAK/DEPLOY GATE - WHAT CAN PROGRESS**
- **LICENCE TO DEPLOY/ DEPLOYMENT WAIVERS**
- **VULNERABILITY RULES**
- **PRODUCTION CHECKS**





OPERATE - MONITOR (PROD)

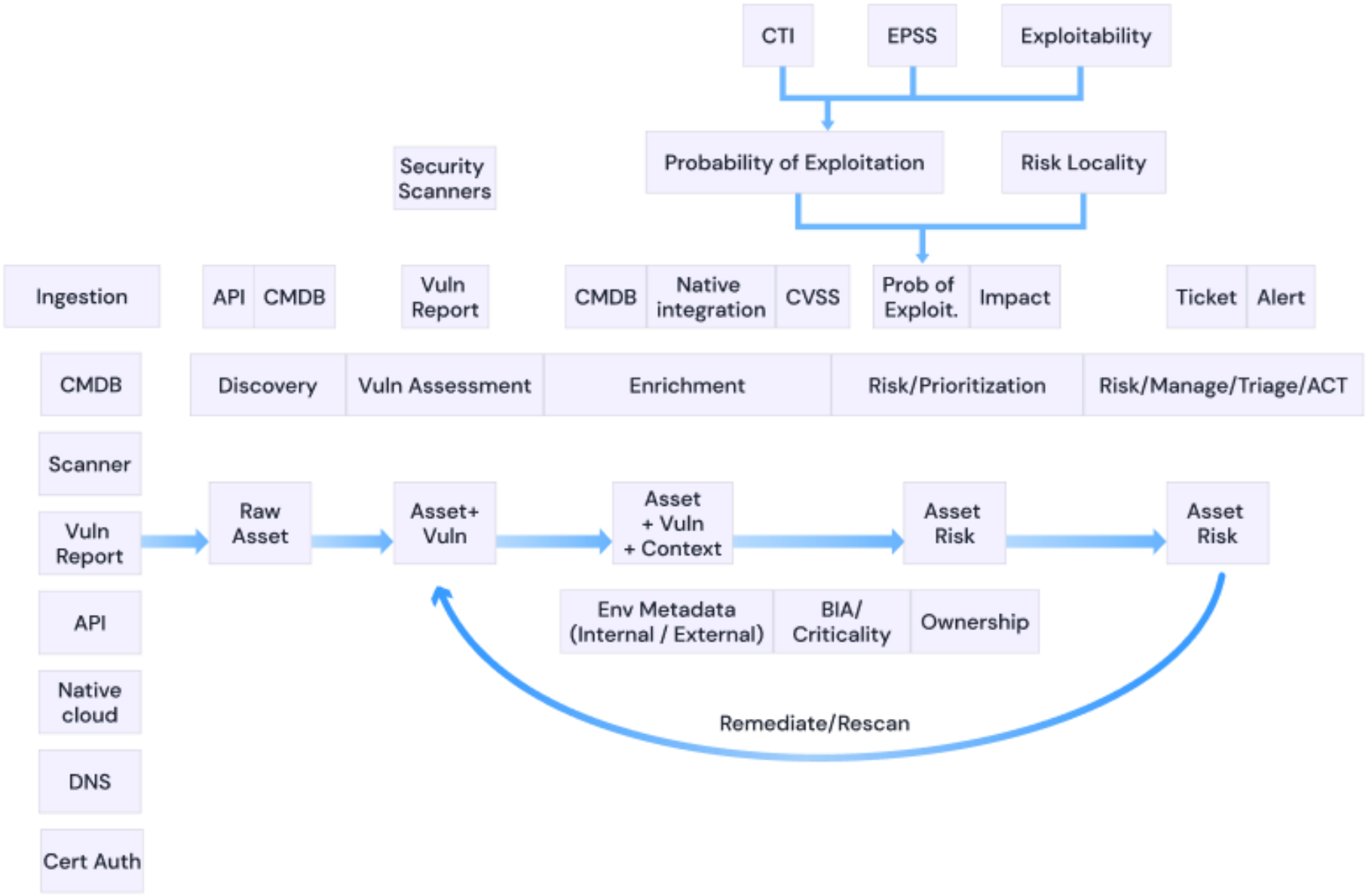
- **CLOUD VULNERABILITIES**
- **INFRASTRUCTURE VULNERABILITIES**
- **CONTAINER VULNERABILITIES**
- **O/S VULNERABILITIES**
- **VULNERABILITIES WITHIN SLA**
- **NEW VULNERABILITIES INTRODUCED**
- **MEAN TIME TO RESOLUTION**



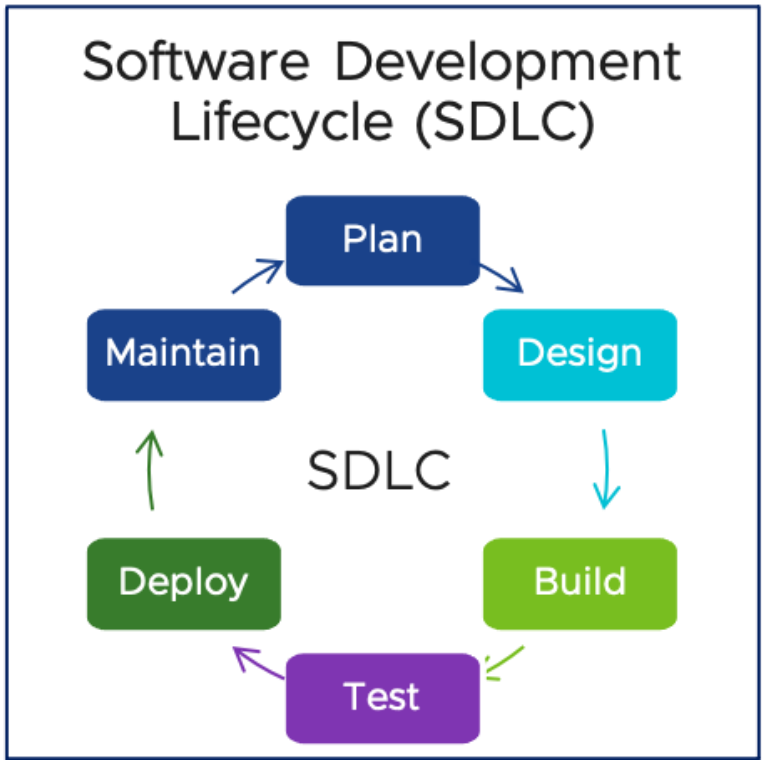
MONITOR

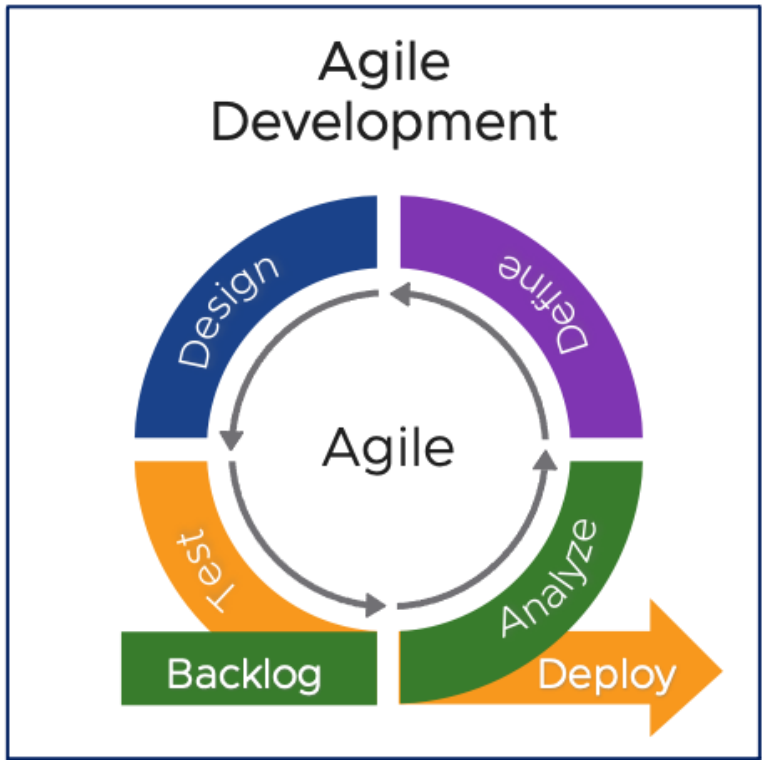
- **CLOUD VULNERABILITIES**
- **INFRASTRUCTURE VULNERABILITIES**
- **CONTAINER VULNERABILITIES**
- **O/S VULNERABILITIES**
- **VULNERABILITIES WITHIN SLA**
- **NEW VULNERABILITIES INTRODUCED**
- **MEAN TIME TO RESOLUTION**
- **BUILD VS FIX**

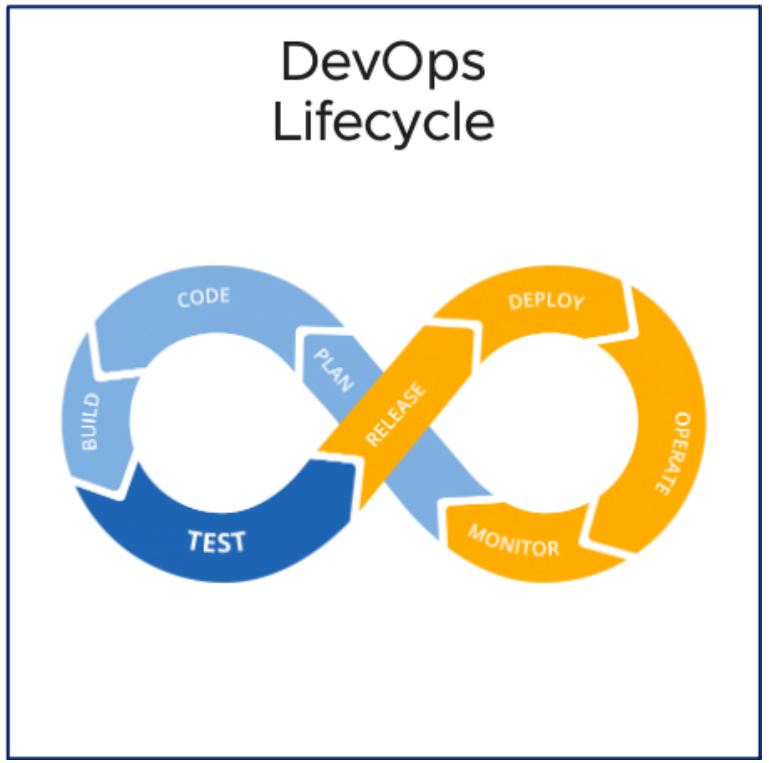
Asset Lifecycle



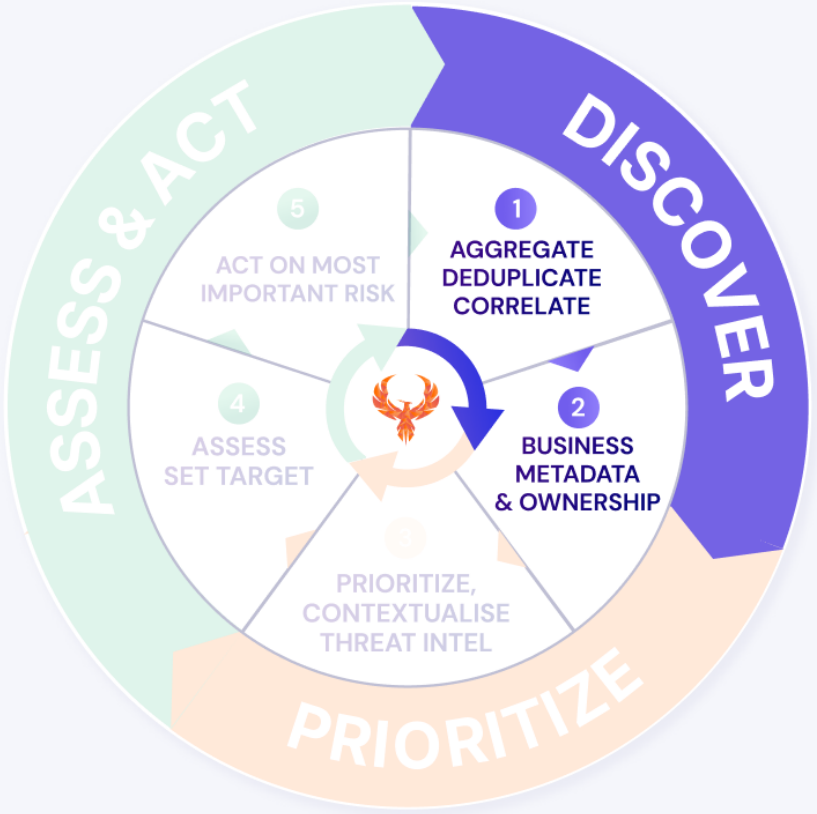
Evolution of Software, Shfit Left vs Shift Right





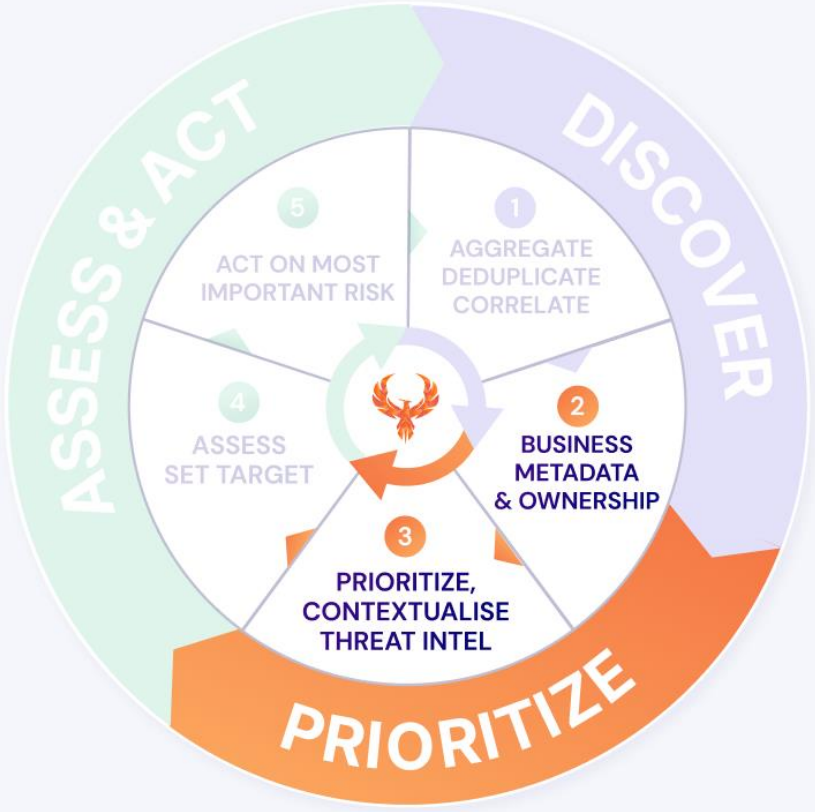


SCOPE, DISCOVER, AGGREGATE



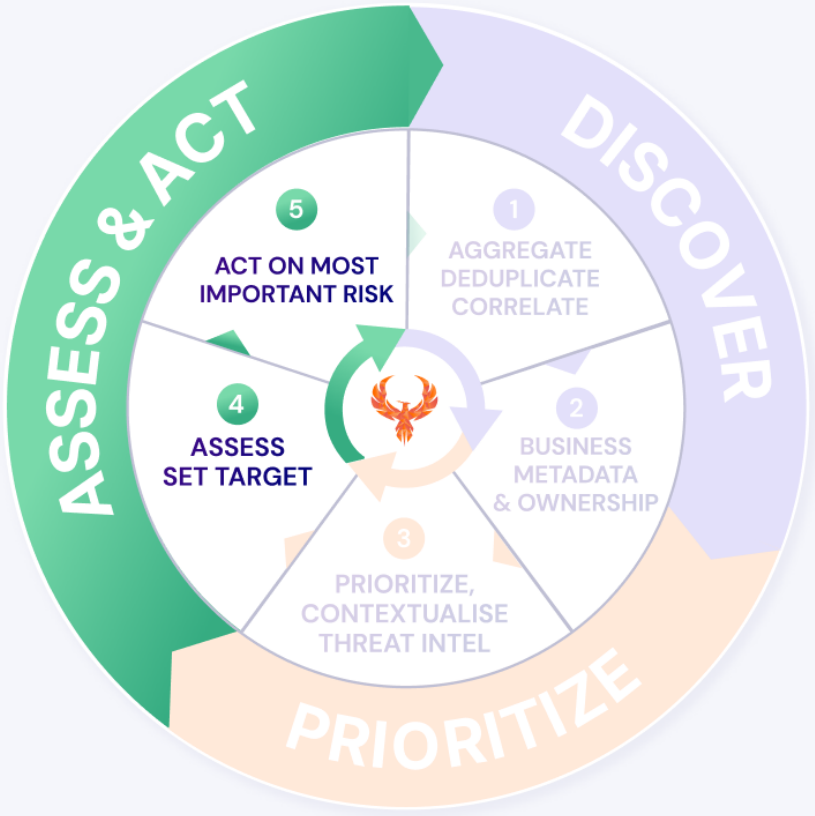
- AGGREGATE ALL THE DATA AND SET BASIC MEASUREMENT
- DISCOVER ASSET POSTURE
- SEGMENT THE ASSET BY BUSINESS AND ADD OWNERSHIP

PRIORITIZE



- PRIORITIZE BASED ON THREAT INTEL (EPSS)
- PRIORITIZE BASED ON CONTEXTUAL AND ASSET LOCATION
- PRIORITISE BASED ON BUSINESS CRITICALITY AND IMPACT

ACT



- ACT ON THE VULNERABILITIES THAT ARE MORE EXPLOITABLE
- SET RISK BASE TARGET AND ACT ON THE VULNERABILITIES TO REACH THE TARGET
- AUTOMATE THE OPENING OF TICKET, MEASURE MEAN TIME TO RESOLUTION

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

RESEARCH TOP 25

Top 10 Vulnerabilities by Popularity:

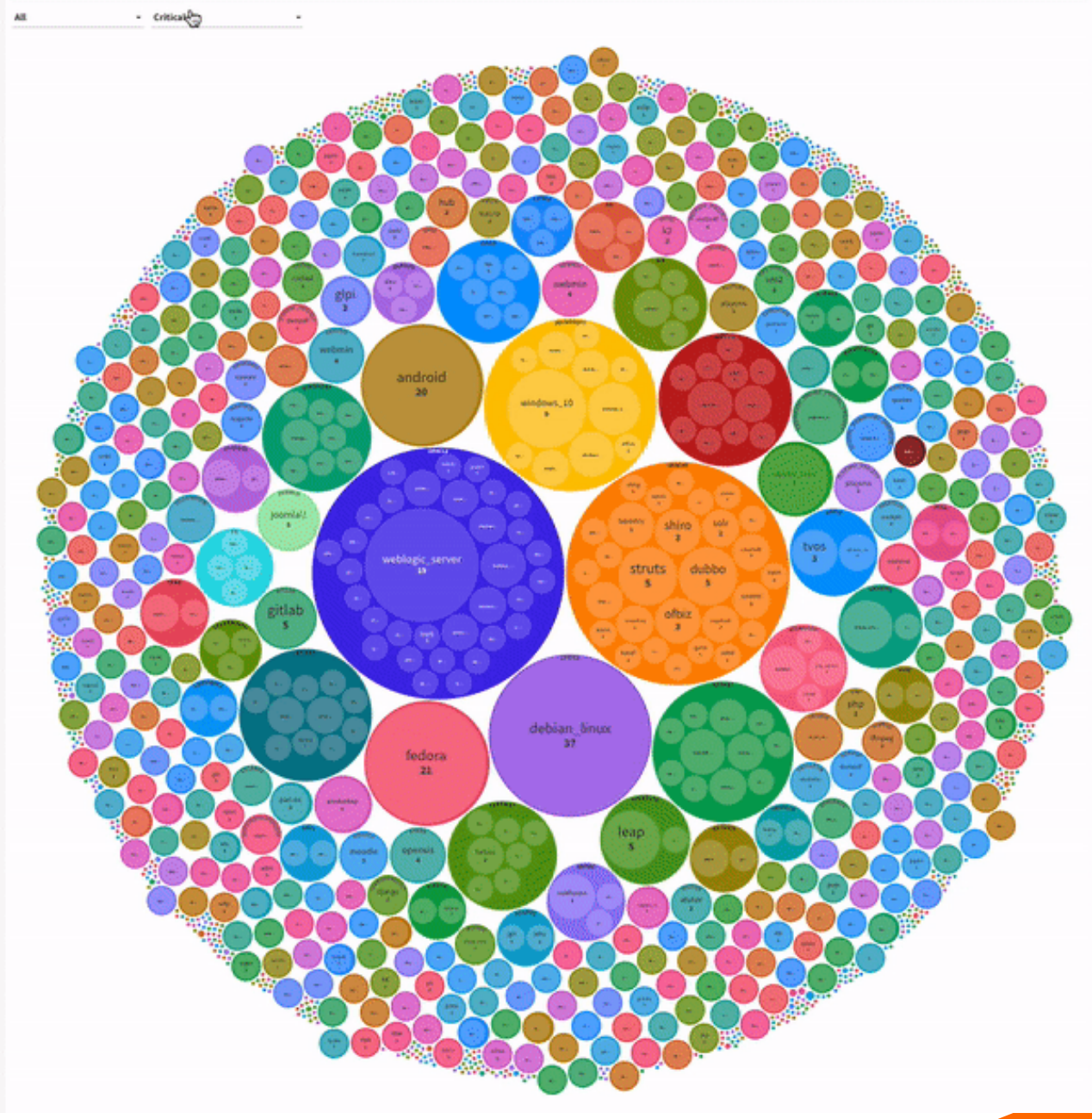
1. Microsoft
2. Oracle
3. Debian
4. Apache
5. Google
6. NetApp
7. Redhat
8. Apple
9. Fedoraproject
10. Atlassian

Top 10 Vulnerabilities by Criticality:

1.Oracle
2.Apache
3.Debian
4.Microsoft
5.Fedoraproject
6.Google
7.Redhat
8.VMware
9.NetApp
10.Zohocorp

Top 10 by Weighted Average EPSS:

1. Oracle
2. Microsoft
3. Apache
4. Debian
5. Redhat
6. Atlassian
7. VMware
8. F5
9. GNU
10. NetApp



https://public.flourish.studio/visualisation/14643482/

https://www.phoenix.security
https://uk.linkedin.com/in/fracipo

@FrankSEC42

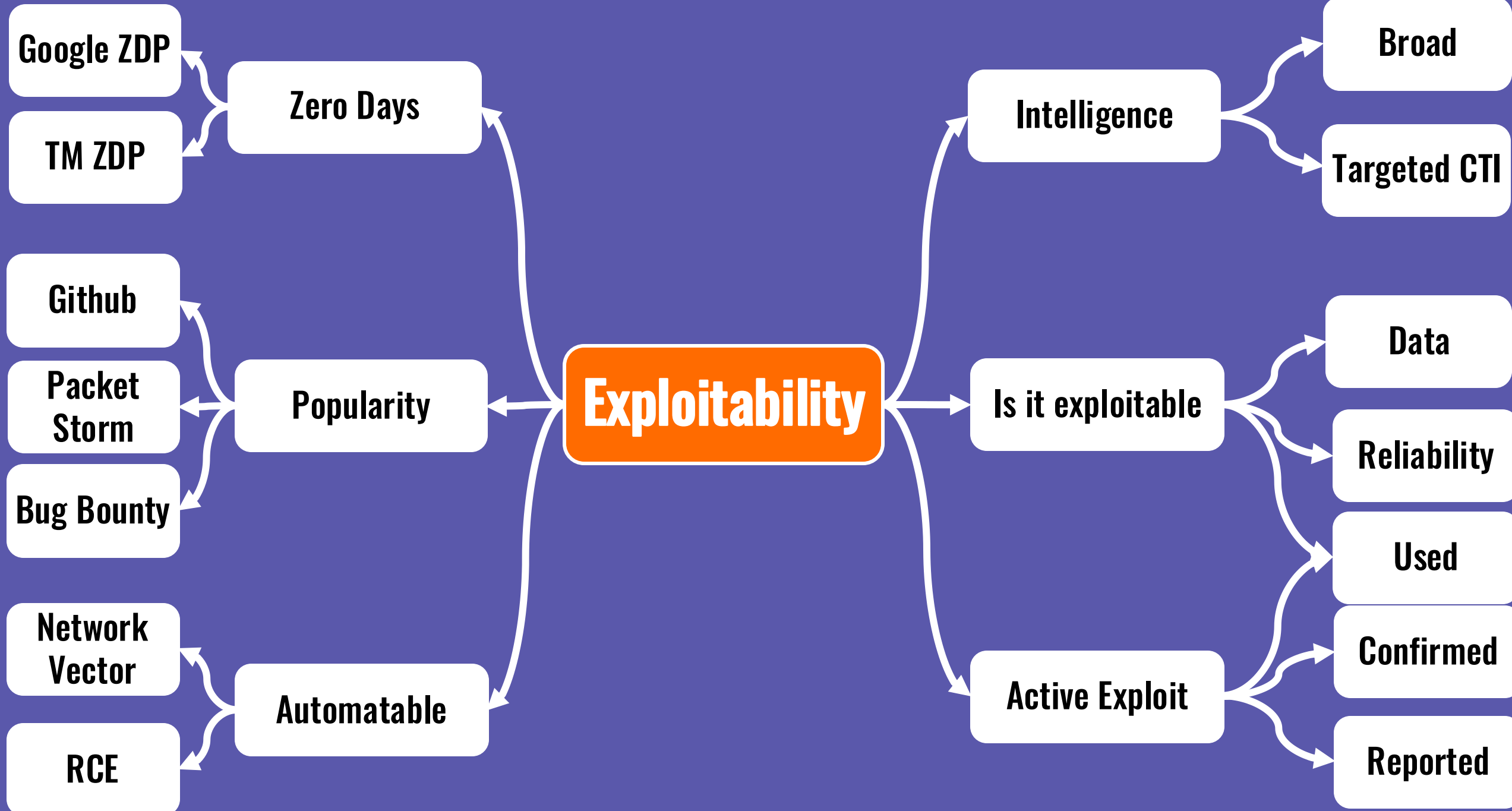
Exploitability in the wild

Github Exploits

NVD Exploits

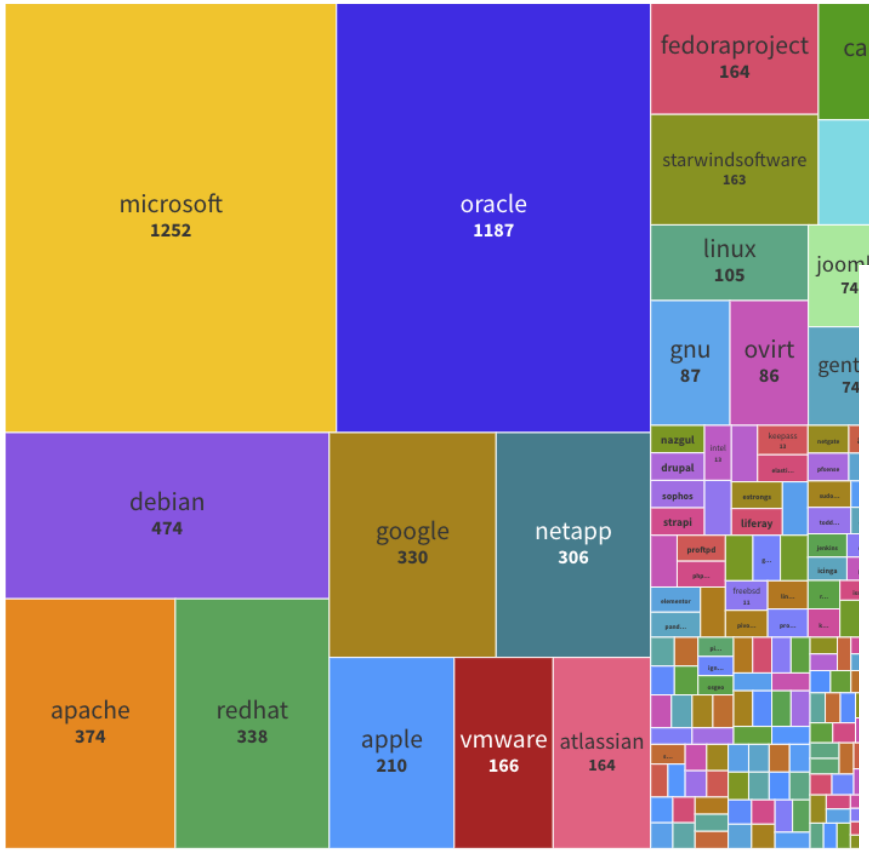
CISA Kev

EPSS

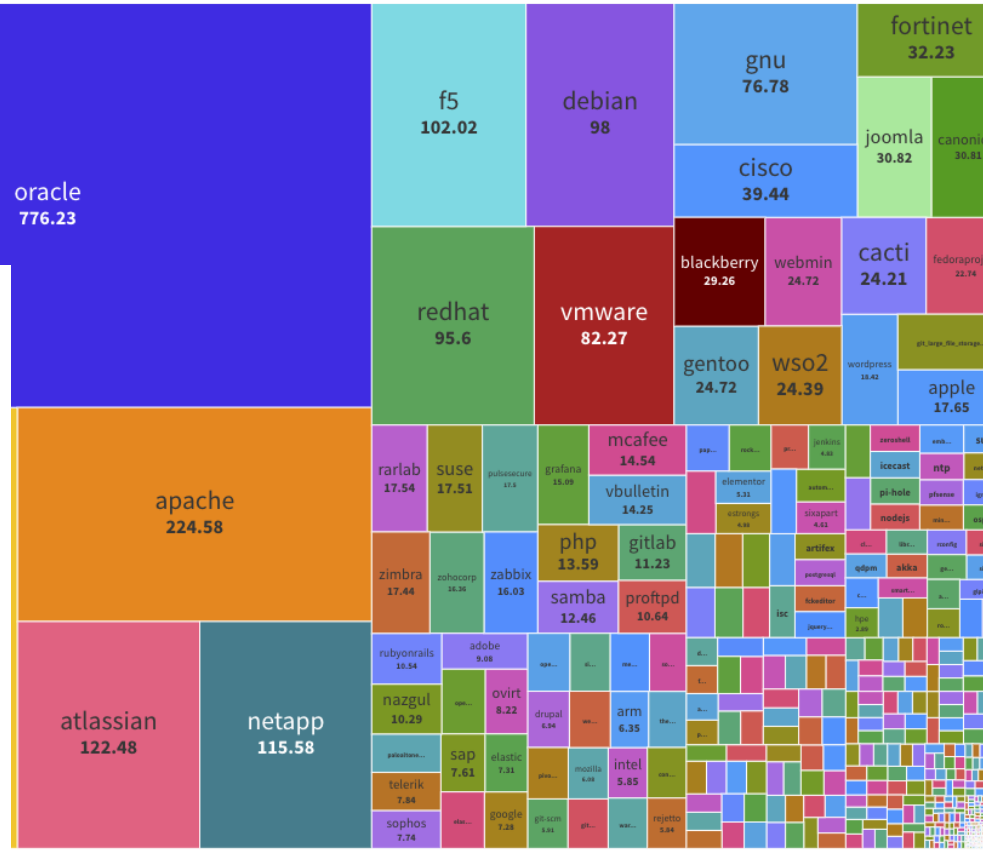

Exploitability
Zero Days
Google ZDP
TM ZDP
Popularity
Github
Packet Storm
Bug Bounty
Automatable
Network Vector
RCE
Intelligence
Broad
Targeted CTI
Is it exploitable
Data
Reliability
Active Exploit
Used
Confirmed
Reported

TOP EXPLOITED VENDOR

Number of Exploits

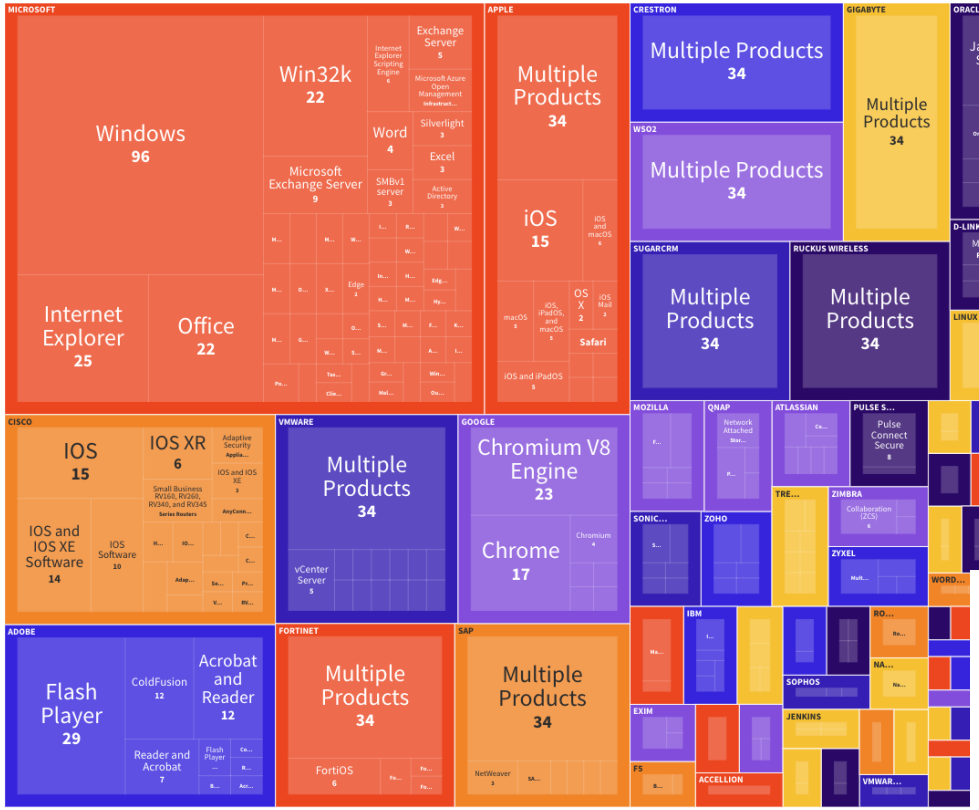


Number of Verified Exploits

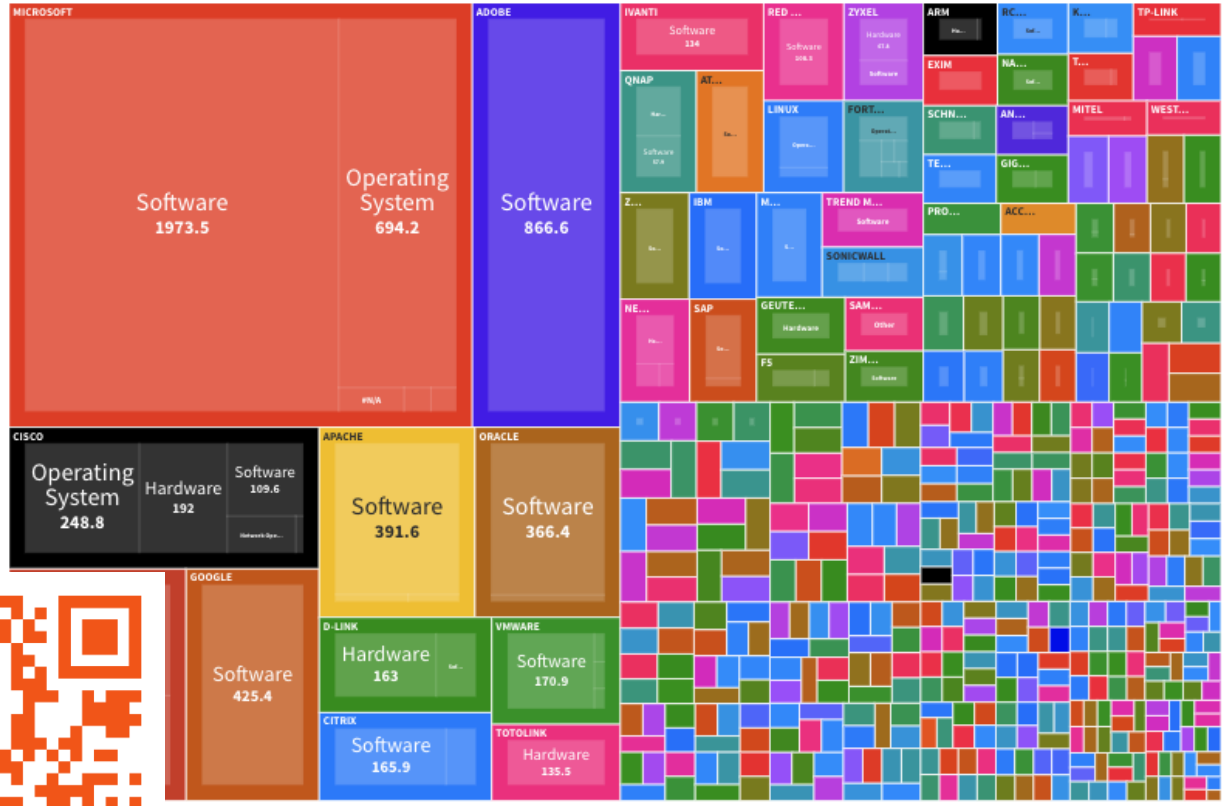


TOP VERIFIED EXPLOITS

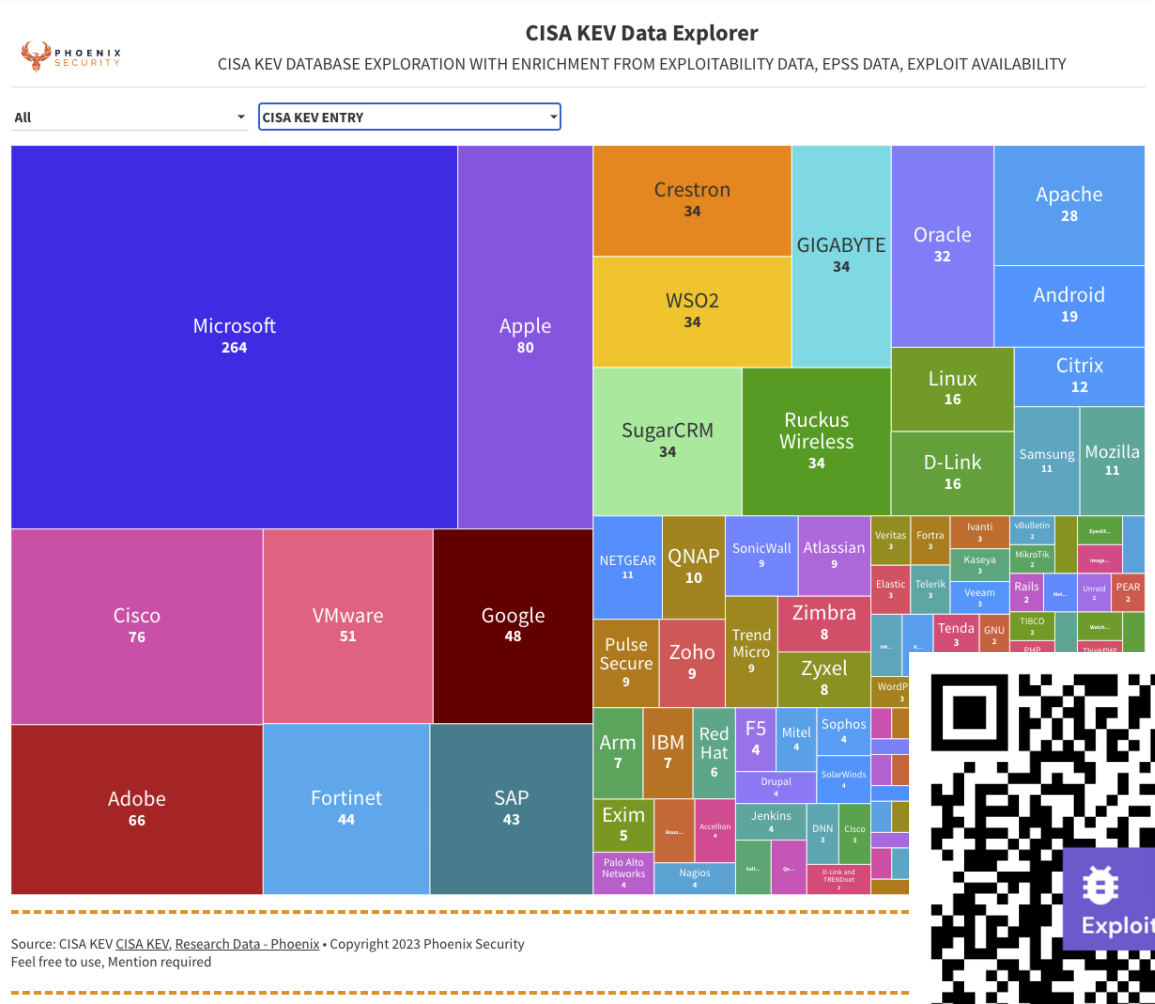
CISA Kev

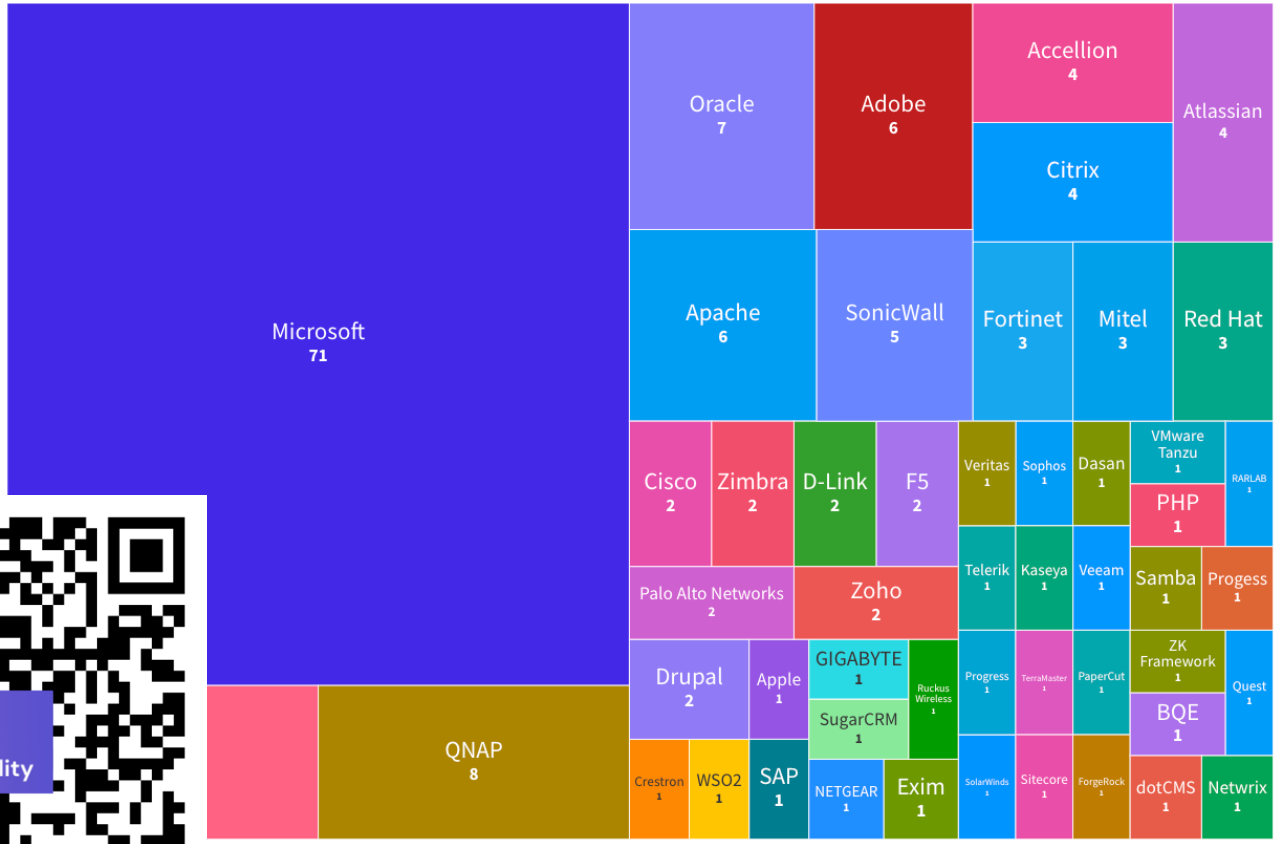


VULN CHECK KEV



Vulnerabilities used in ransomware

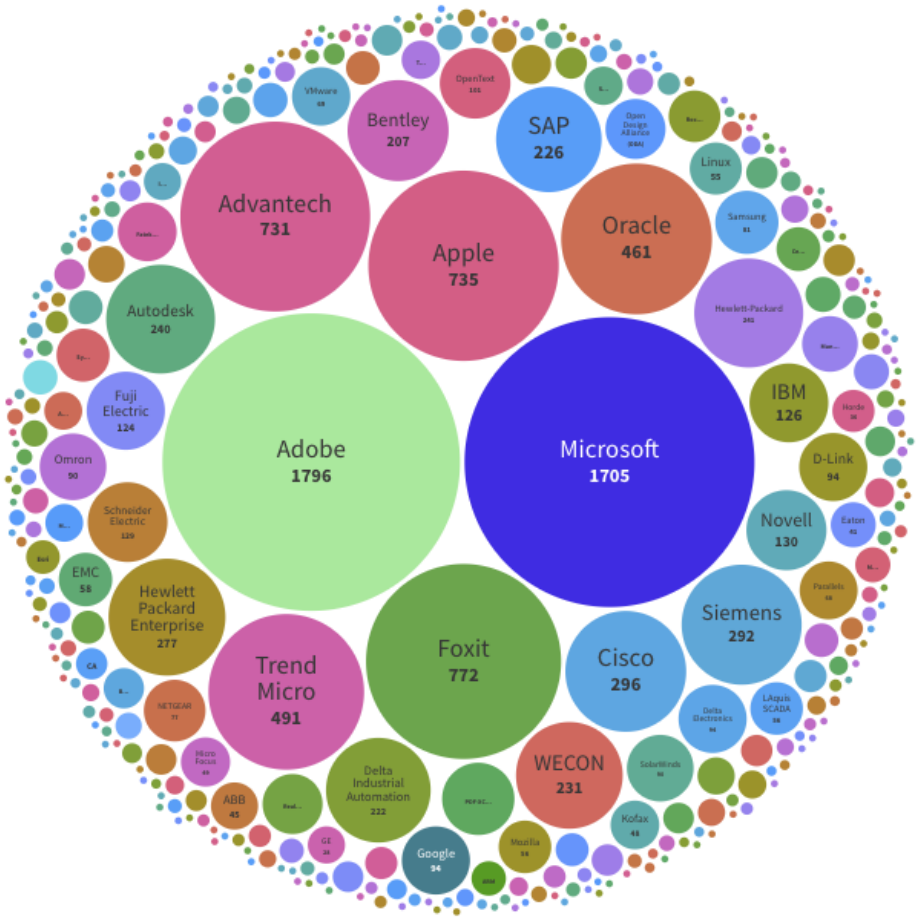


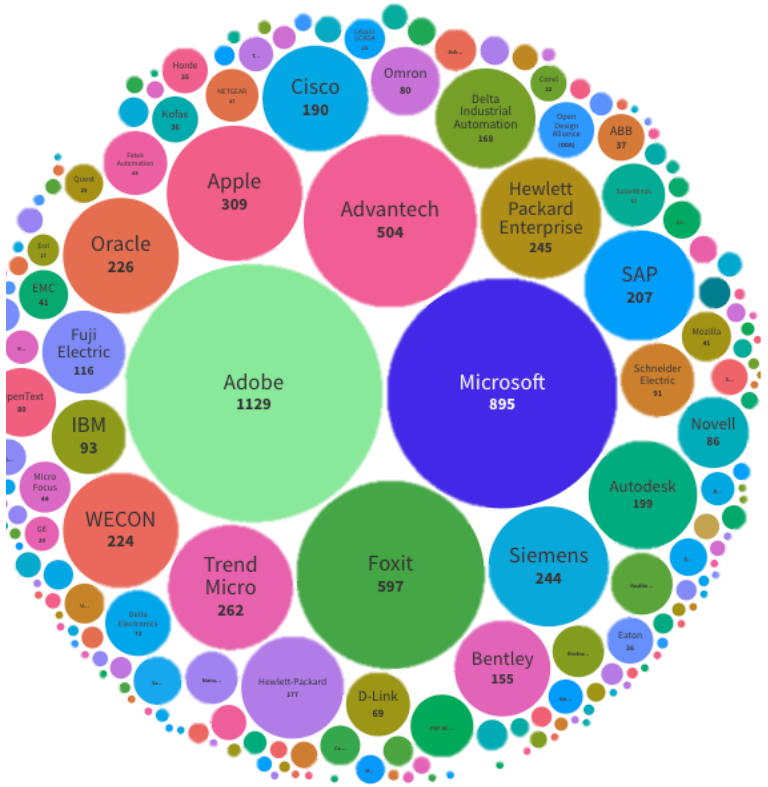


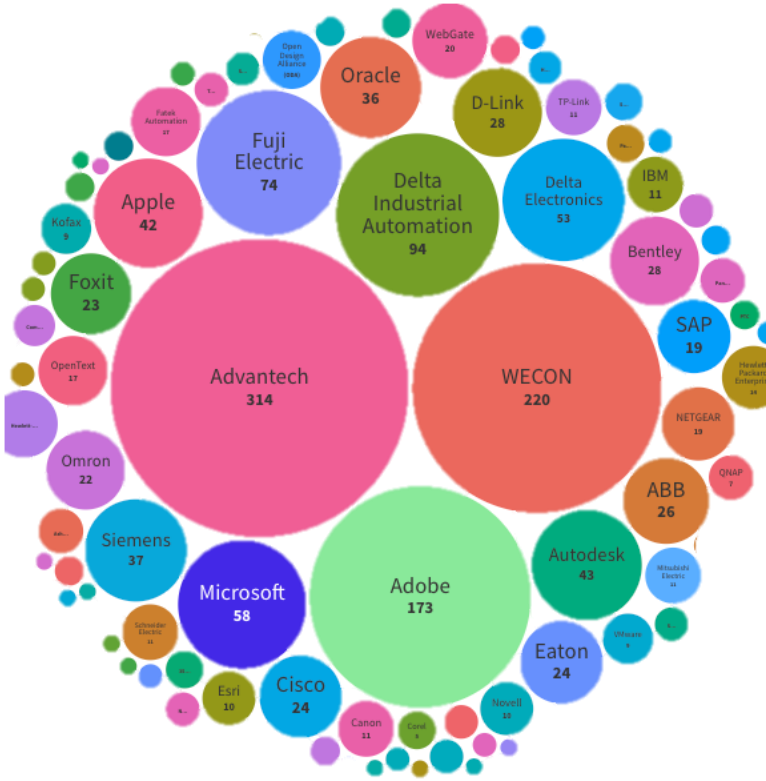
Vendor with most ZERO DAY

Exploitability

Buffer Overflow

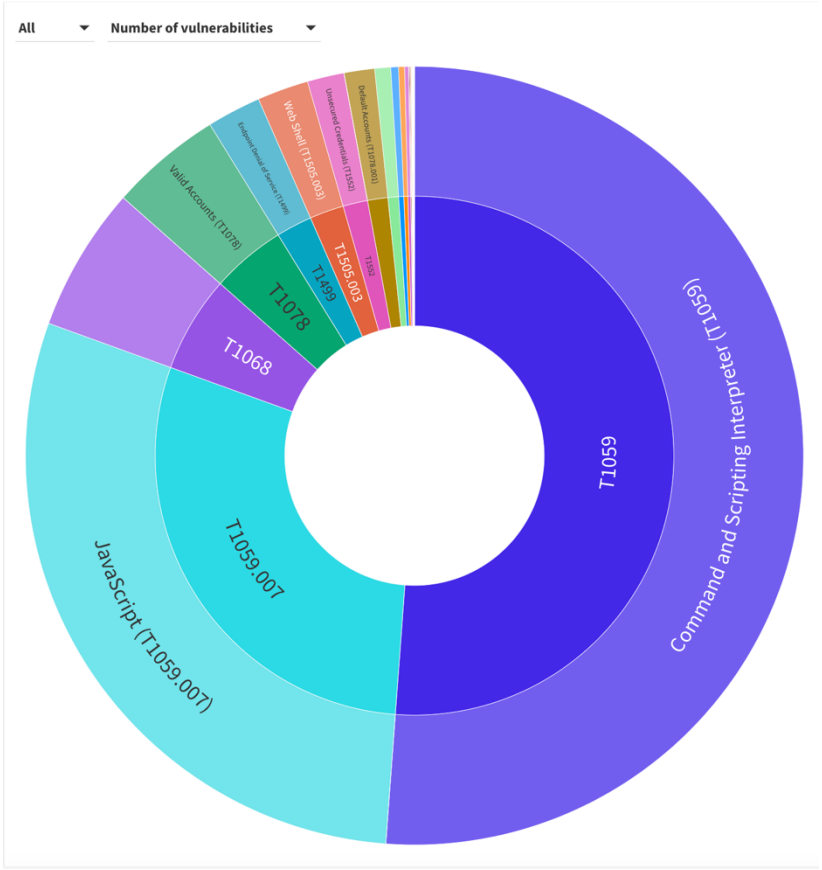




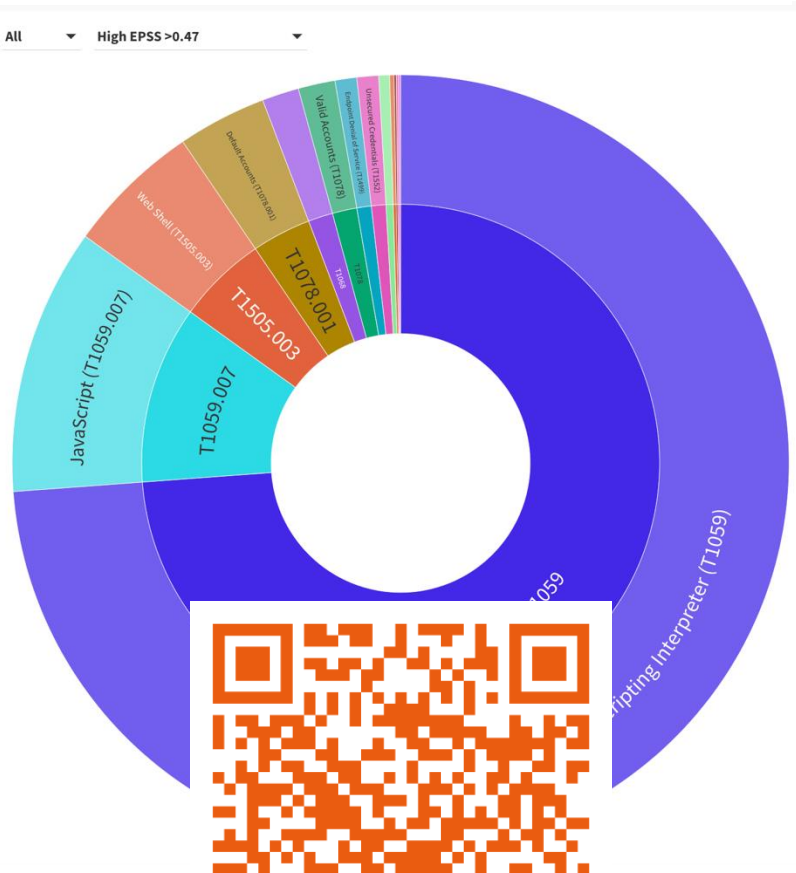


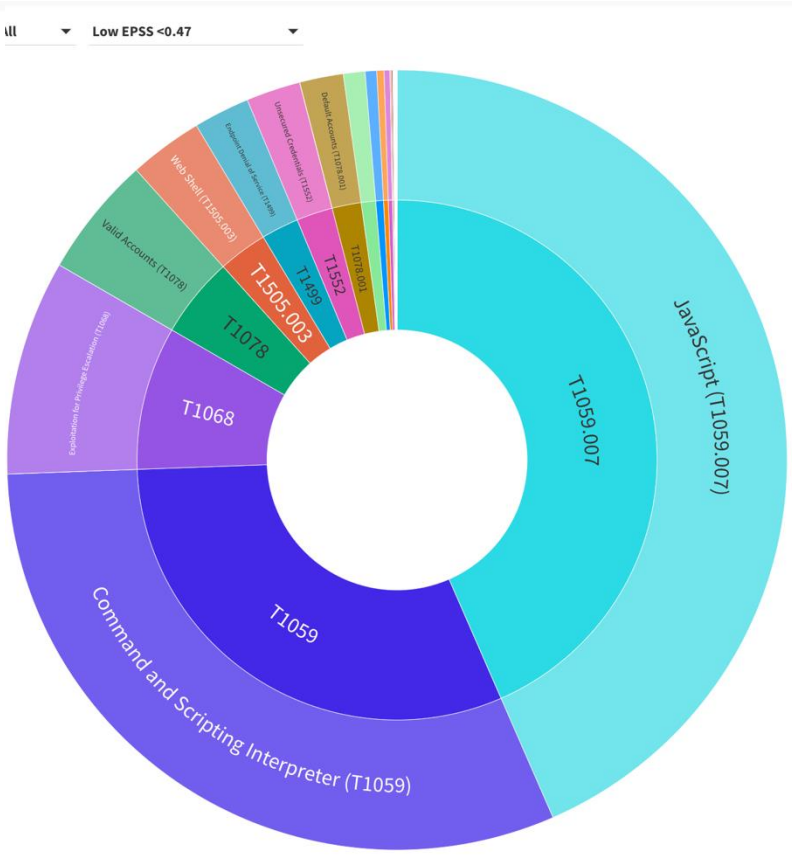
RCE

Most Used MITRE & ATACK Techniques



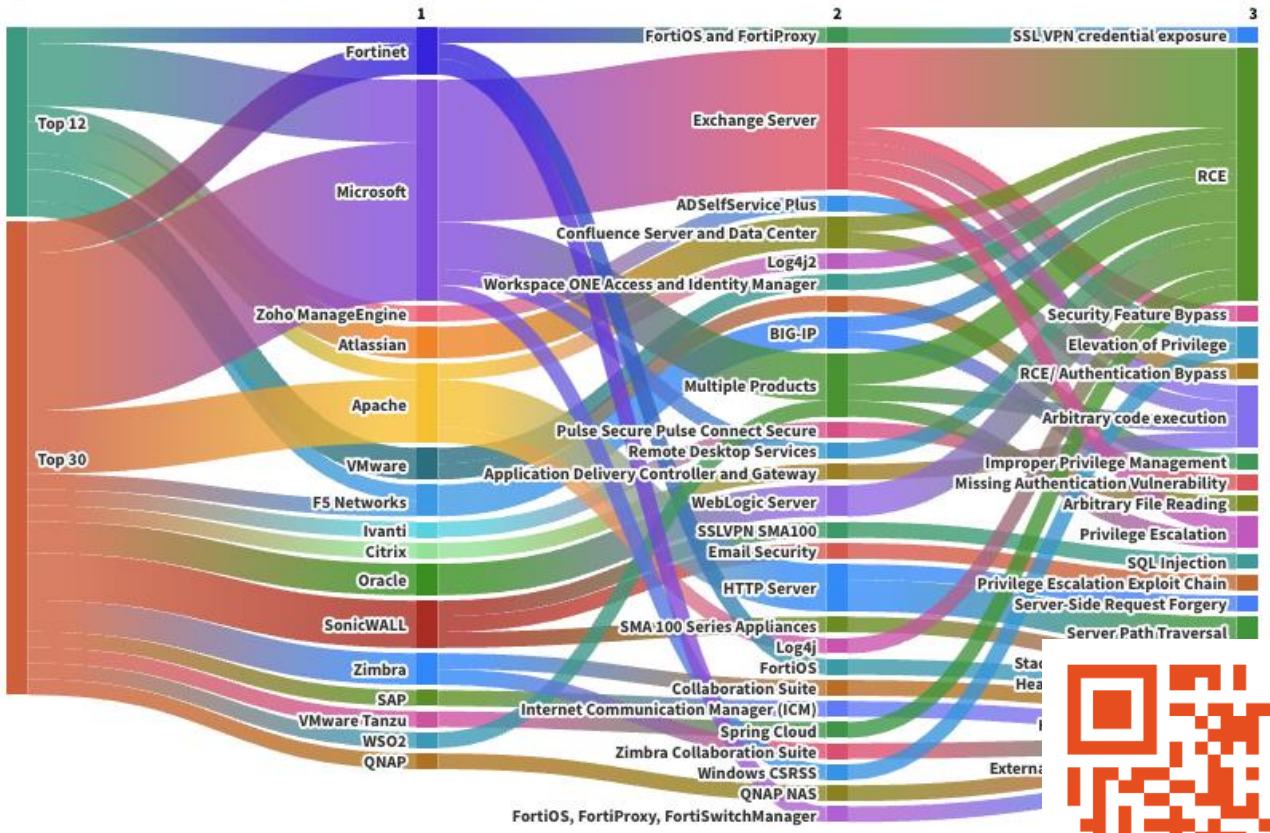
HIGH EXPLOITABILITY LOW EXPLOITABILITY





MOST USED ATTACK METHODS

TOP EXPLOITS METHODS



CISA KEV