Building resilient Application security programs

APPLICATION SECURITY VULNERABILITIES - MEASUREMENTS, MATURITY MAGIC - VULNERABILITY FRAMEWORK PROJECT

PHOENIX SECURITY

Aggregate
Contextualize
ACT

Francesco Cipollone, Founder
fc@phoenix.security

Warning

About Francesco

Francesco Cipollone

Founder Phoenix Security, Chair CSA UK

I'm a cloud expert and have been a CISO Advisor, Cybersecurity Cloud Expert. Speaker, Researcher and Chair of Cloud security Alliance UK, Researcher and associate to ISC2.

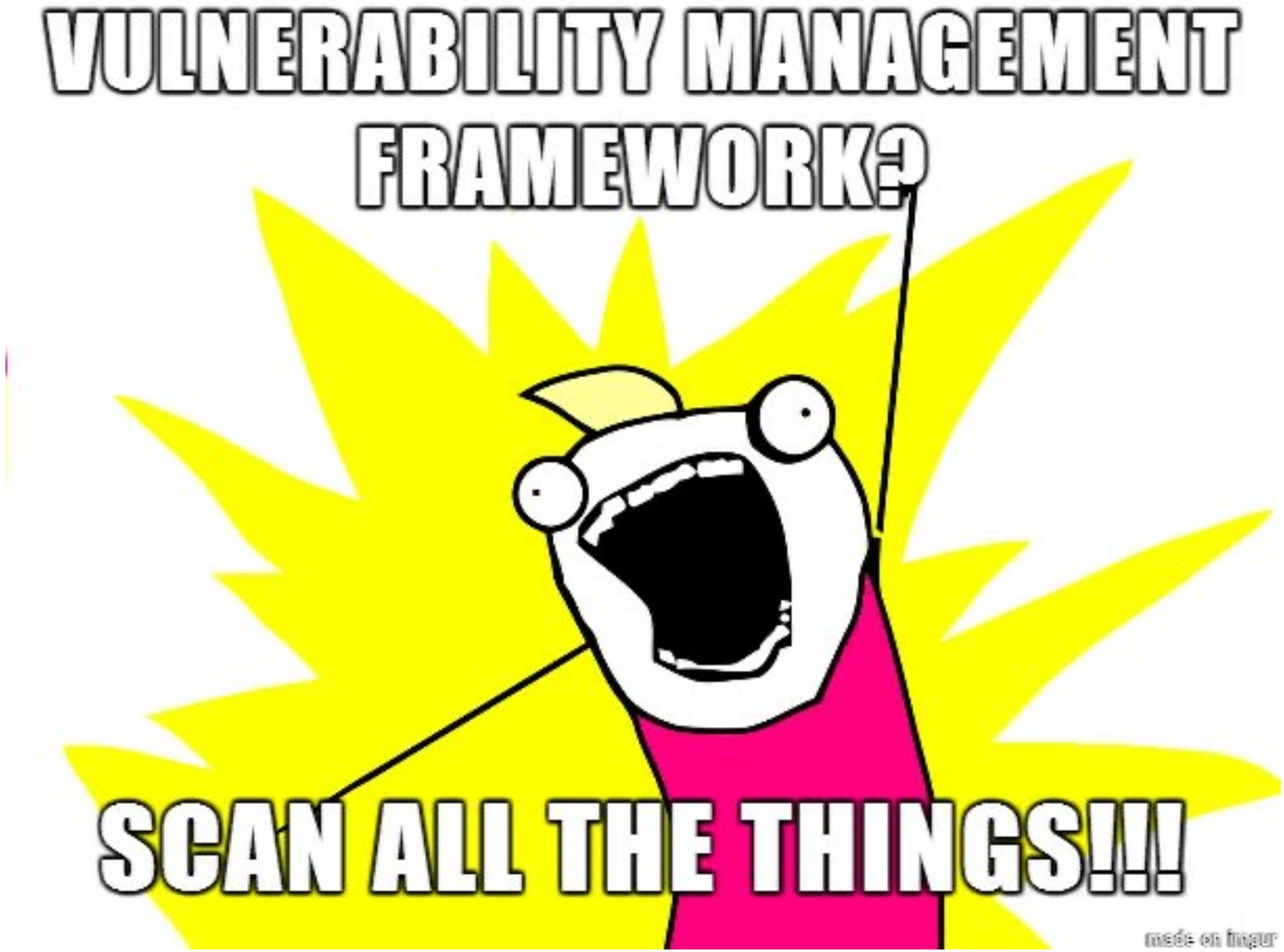
Currently we are working on interesting problem on how to link Application, Security and

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

Prevent Burnout is key to happy living

Can we scale security to make it more enjoyable?

Been Warned



Agenda

- Intro & Context
- Problem of vulnerabilities
- Security-developers WHO needs to triage?
- Human cost of fixing manually
- Appsec Security Framework
  - Modern SSDLC
  - Triaging and Reporting
  - Vulnerability Framework
- Recommendation/ Conclusion
- Q&A

Why do we need it?

The first challenge … and it’s getting worse

SLOW DEFENDER

40/ 100-150 days

Average time to fix a vulnerability

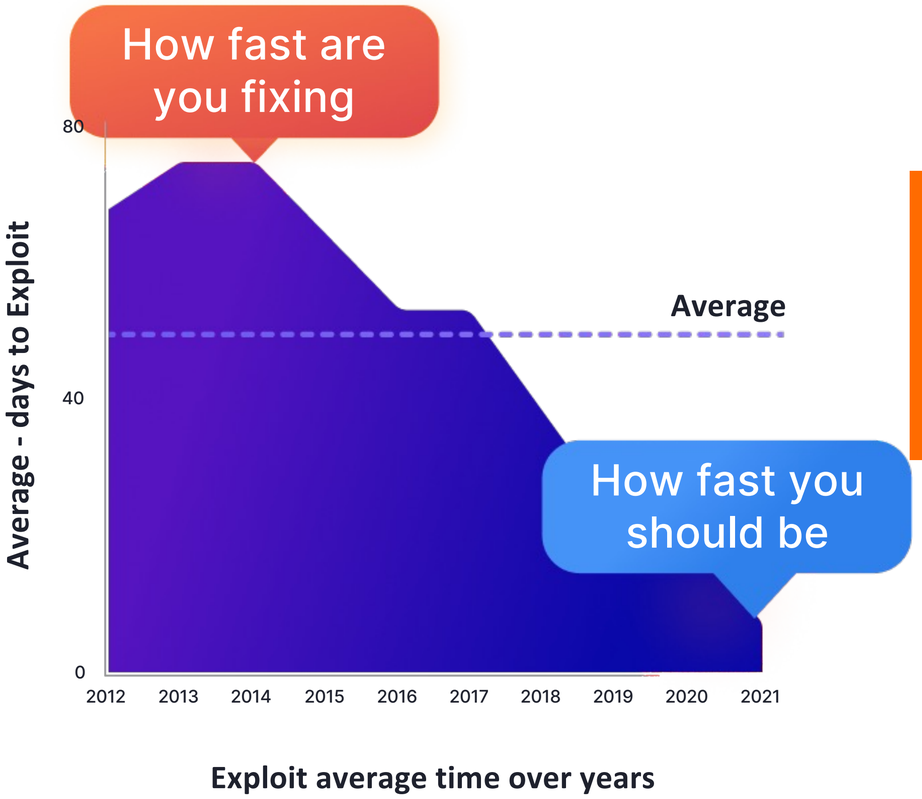
FAST ATTACKER

3-15 days

Average time to exploit a new vulnerability

WHY IS IT IMPORTANT? – MORE ASSETS LESS TIME

1:4 BREACH DUE TO VULNERABILITY

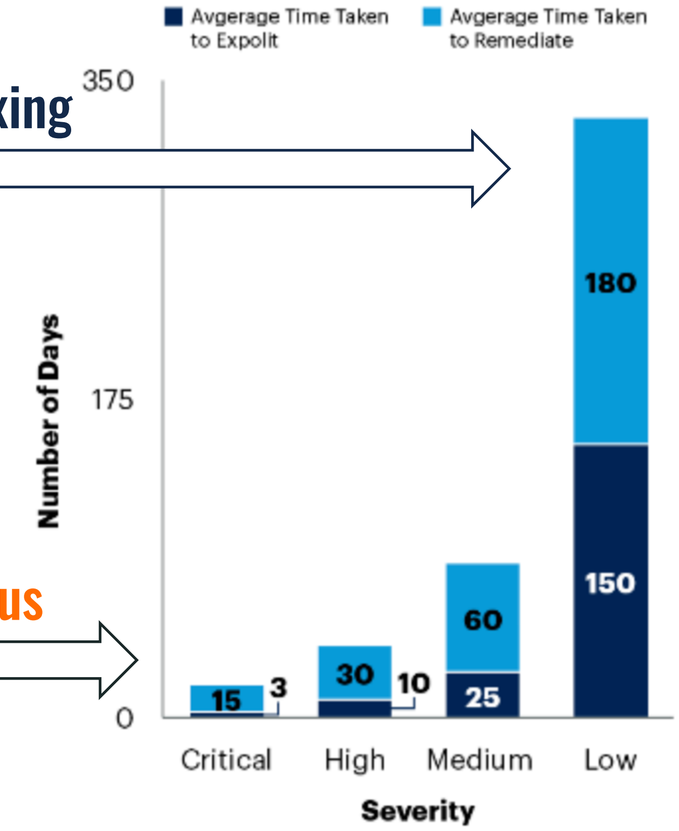


Exploit average time over years

2013 defense with 2023 attackers

How fast are you fixing

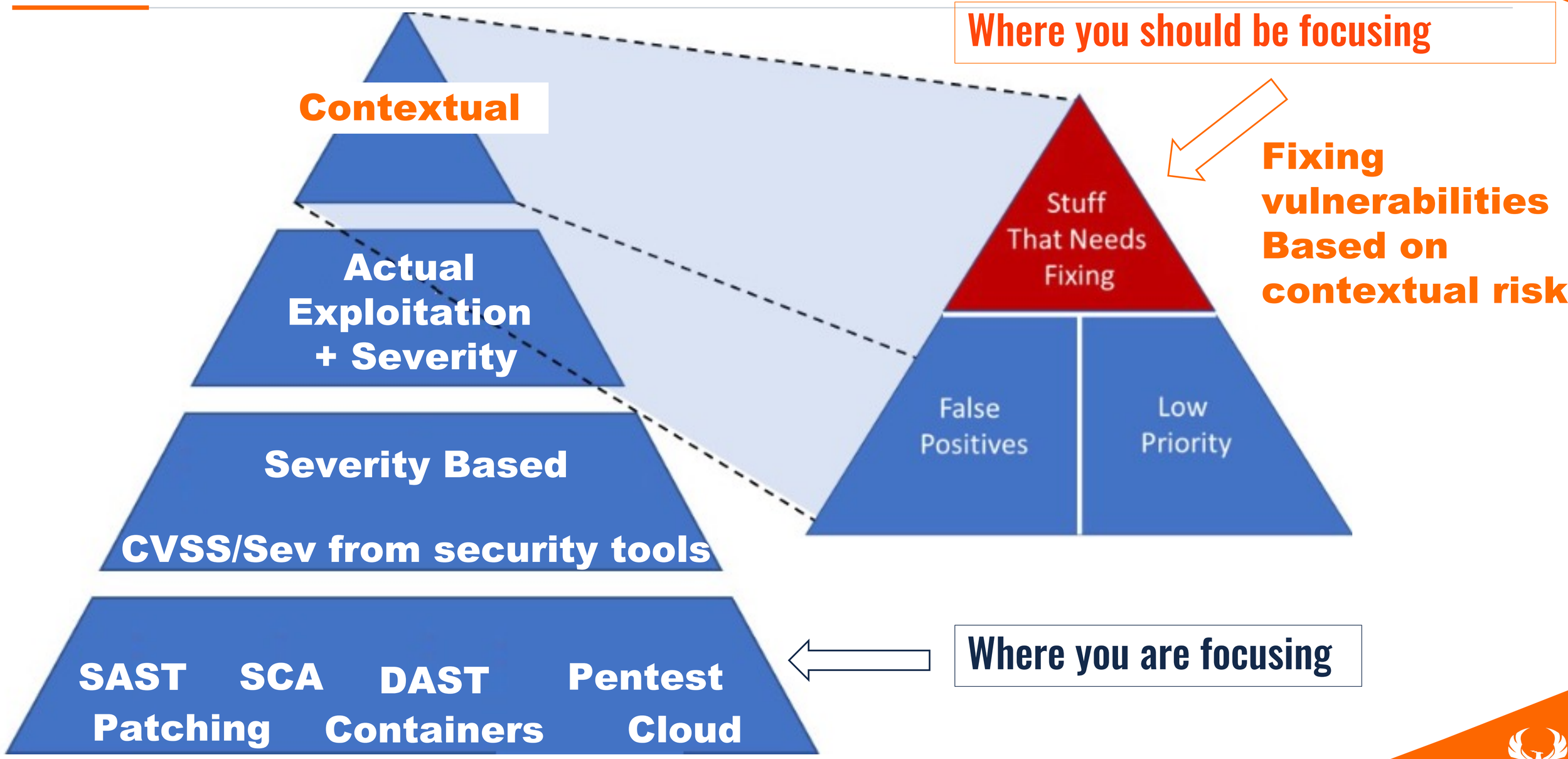
Where you should focus



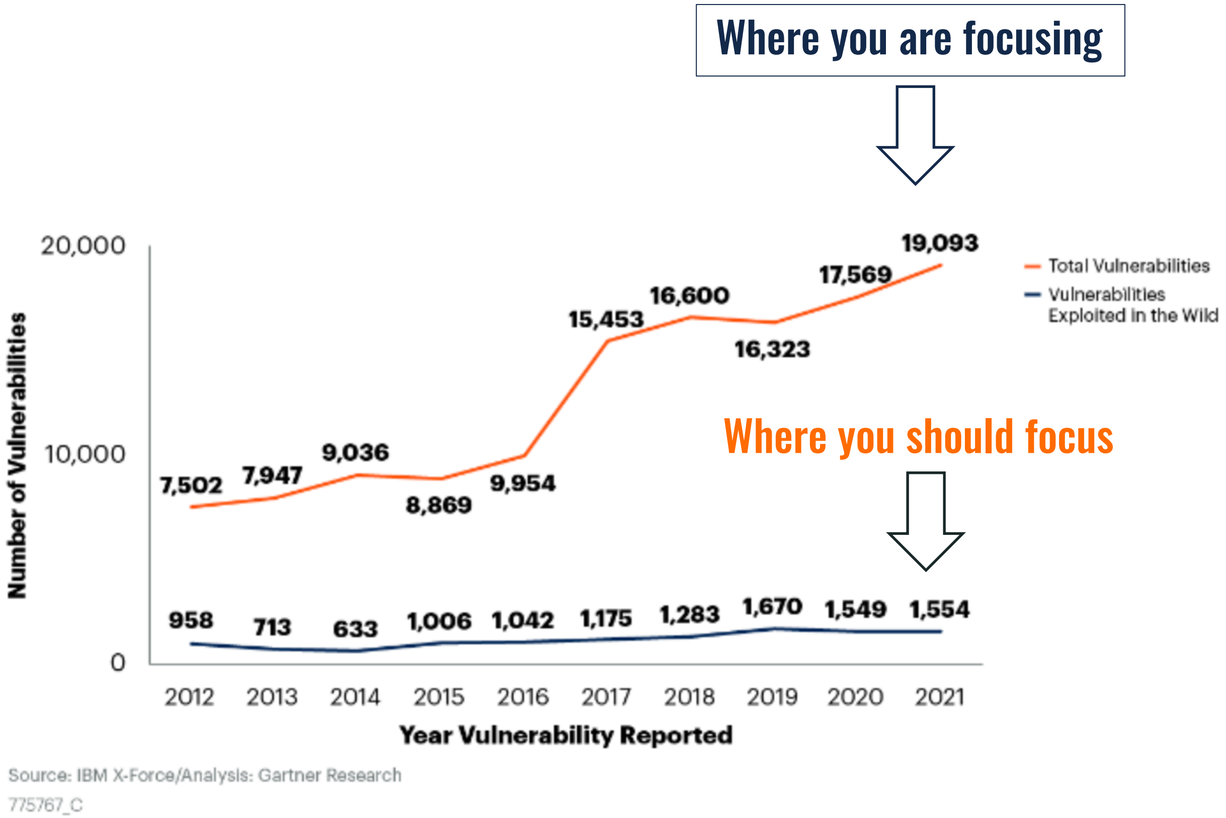
Source: Gartner
760501_C

Source gartner: https://www.gartner.com/document/code/775767

Prioritization is so 90....



WHY IS IT IMPORTANT?



34% More Vulnerabilities Every year

10% are actually important

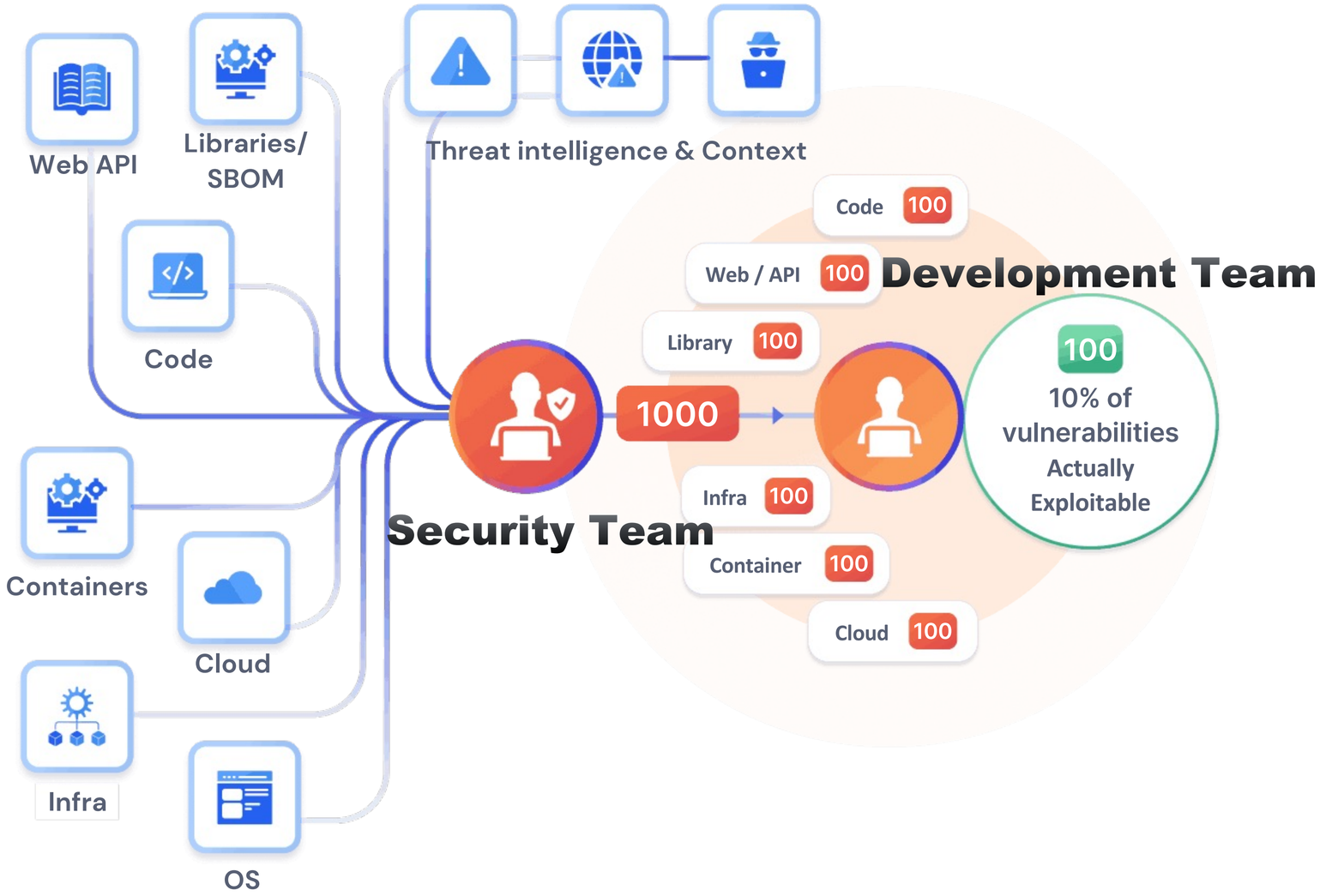
How do you get there?


Who Should fix
What is the most
urgent?
3RD PARTY LIBRARIES
3RD PARTY LIBRARIES
THREAT INTELLIGENCE & CONTEXT
APPLICATIONS
O/S
OEM SOFTWARE
3RD PARTY LIBRARIES
API/ WEB
APPLICATIONS
OEM SOFTWARE
INFRASTRUCTURE VM/LAPTOPS
CODE
CODE
ENDPOINTS
CONTAINERS
MISCONFIGURATION
CLOUD
APPLICATIONS
CREDENTIALS
SECRETS
LIBRARIES
O/S
CLOUD WORKLOADS
CLOUD WORKLOADS


Needle in a haystack - > But the haystack is on fire

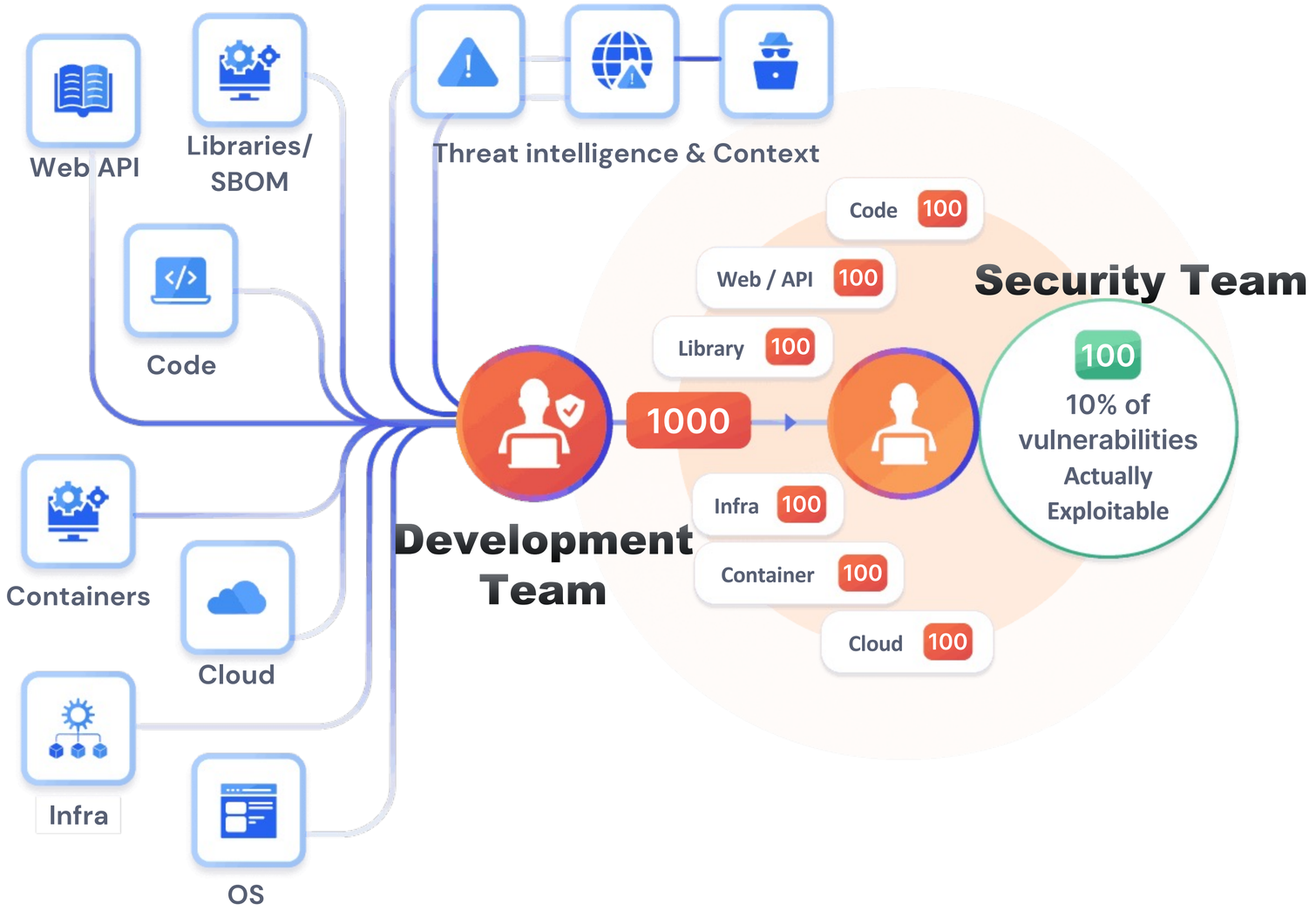
How are we solving it so far...

Security Team Triaging



What's most important – the log4j case

Development team Triaging



What's the solution of this? Opening tickets to dev teams

Driving back home after printing out the vulnerability scan report

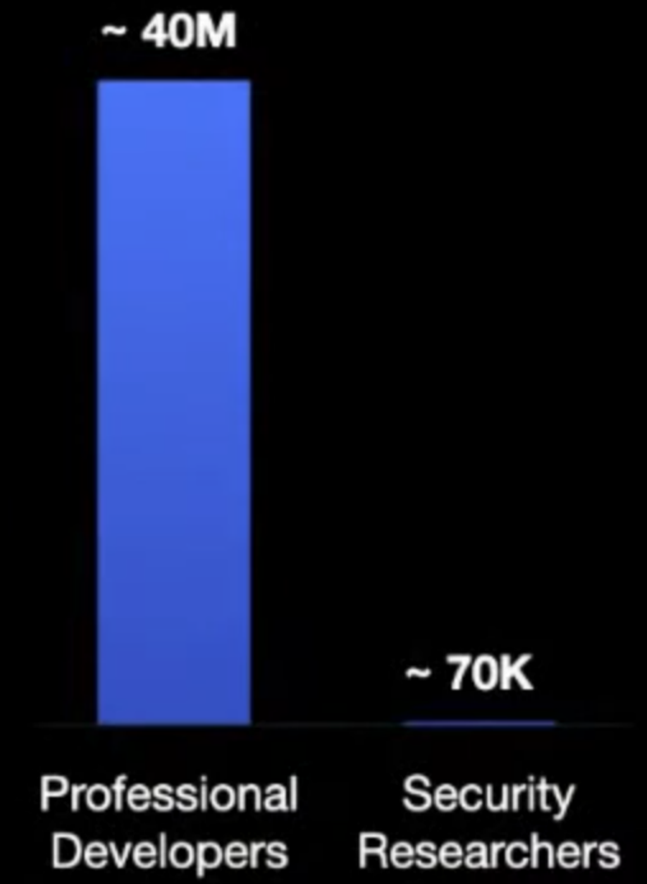
What's most important

Road to burnout

Security researchers are outnumbered!

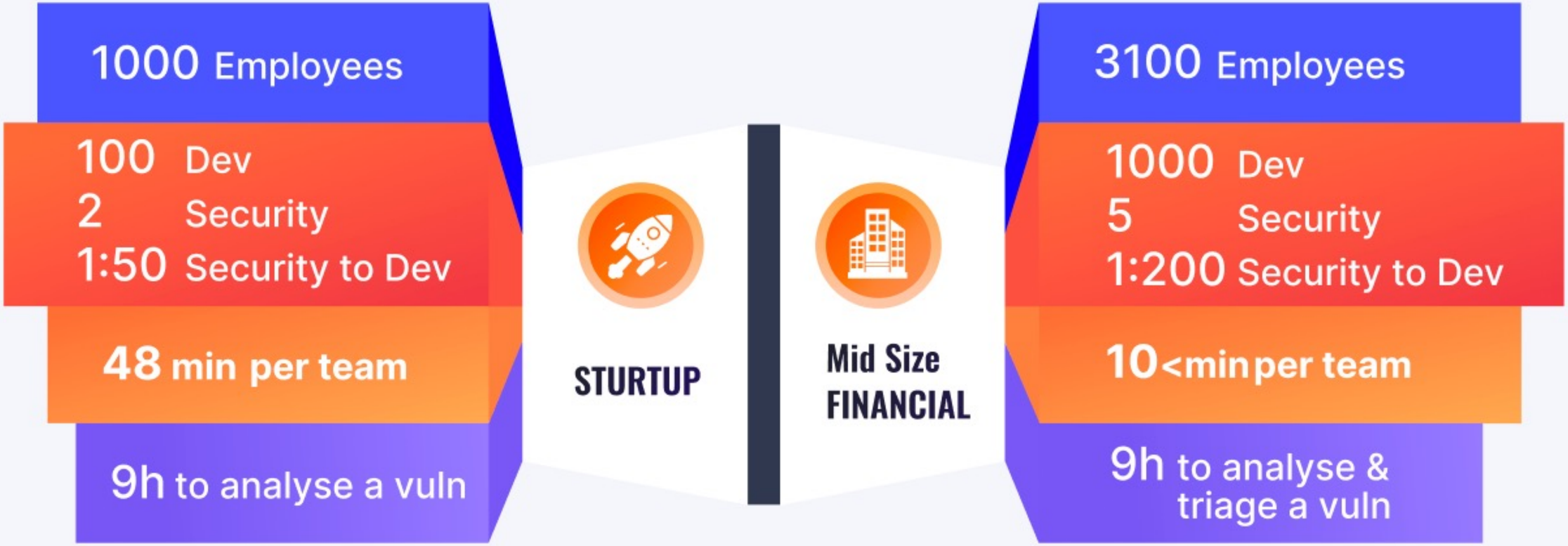
570x

more developers than security researchers



Sources: NIST, Polemon Institute

Regardless Can we solve this problem just with people?



I FEEL YOUR PAIN

BEEN THERE

DONE THAT

ROAD TO BURNOUT

Shift Left?

We're Shifting Everywhere.

Sage Security Champions Conference 18-20 April.
#GoodCleanSecureCode
#ShiftingEverywhere

Shift up shift down
shift left shift right

Sage

COLLABORATE DEV, SECURITY OWENR

3rd person at the table :Audit/Regulation

WHY? Regulation are here and more are coming

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

ISO 27001

PCI DSS COMPLIANT

National Cyber Security Centre

FCA FINANCIAL CONDUCT AUTHORITY

GLBA Gramm-Leach-Bliley Act

Gramm-Leach-Bliley Act COMPLIANT

HIPAA

The NIST Cybersecurity Framework

WHY? Regulation coming

- **Show me the latest vulnerabilities**
- **Show me the vulnerability trends**

- **When did you pentest this application**
- **What are the risk acceptance for this application**
- **When was the last scan**

- **How much time/Effort?**

WHY? Regulation are here...and more coming

- **Requirement 6.1 of PCI DSS** states that organizations must "establish a process to identify…and assign a risk ranking to newly discovered security vulnerabilities."
- **Article 32 of GDPR** requires the implementation "of appropriate technical or organizational measures to ensure a level of security appropriate to the risk."
- The **HIPAA Security Rule** mandates an "assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information."
- The **GLBA Safeguard Rule** requires organizations to "identify and assess risks to customer information…and evaluate the effectiveness of current safeguards for controlling these risks."
- EU Directive on measures for a high common level of cybersecurity across the Union (NIS2) and Cyber Resilience Act (CRA)
- Cyber Resilience Act (CRA) - Manufacturers shall have appropriate policies and procedures, including coordinated vulnerability disclosure policies, referred to in Section 2, point (5), of Annex I
- NCSC guidance on regulation

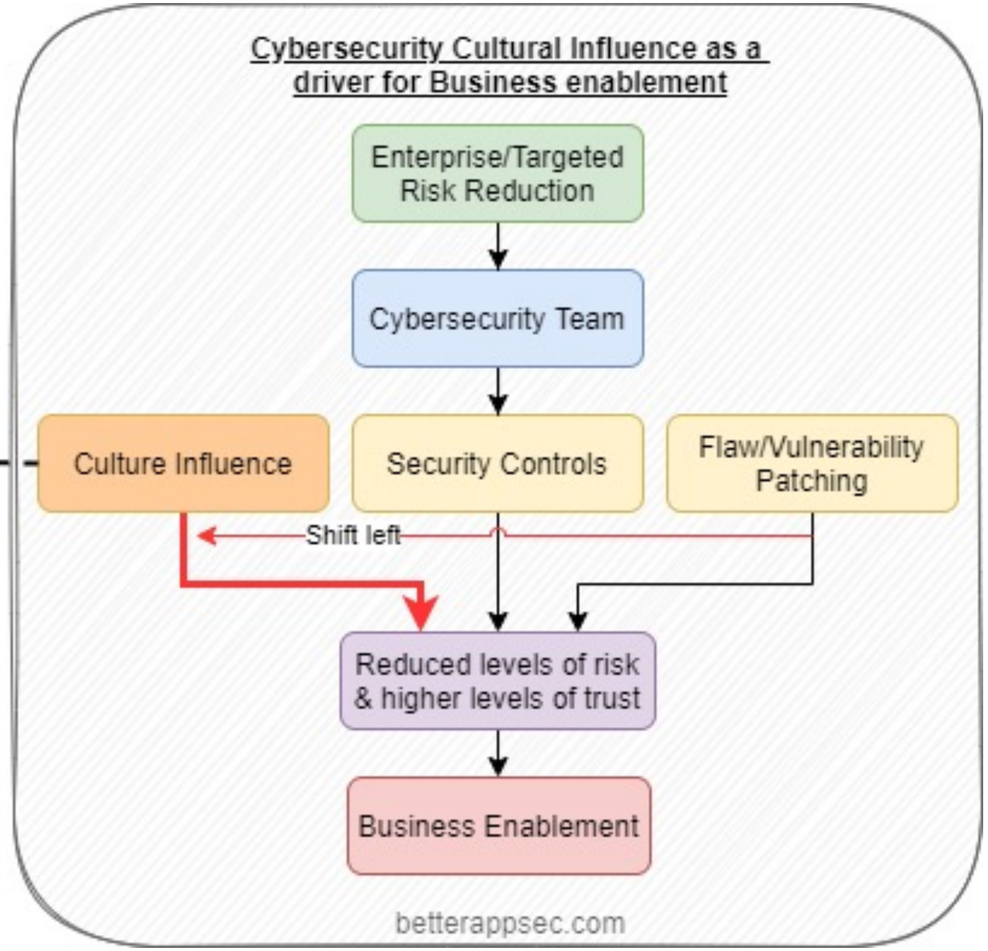
WHAT IS THE OBJECTIVE OF SECURITY?

Objective of security -> Business Enablement

Made of several aspect

- **Influencing people**
- **Fixing as soon as possible**
- **Shift left (don't create issue in first place)**
- **Controls**

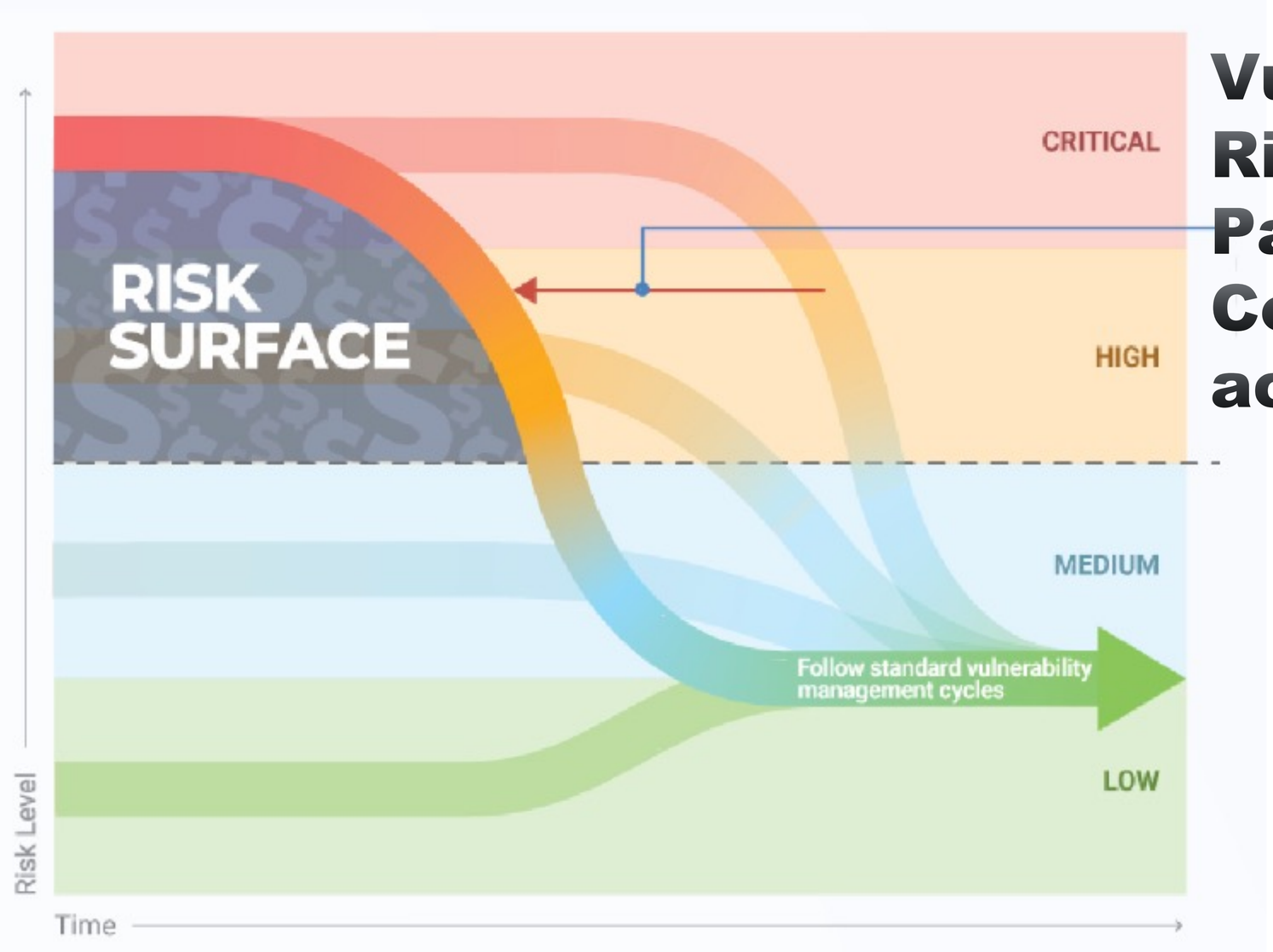
Product/Security Partnerships
Security Guardrails
CI/CD Security Tooling
Security Engineering Innovation



Ultimate Objective
Operate at a business risk lever the organization is comfortable with

Vulnerability is not risk

Risk provide better context than just cvss



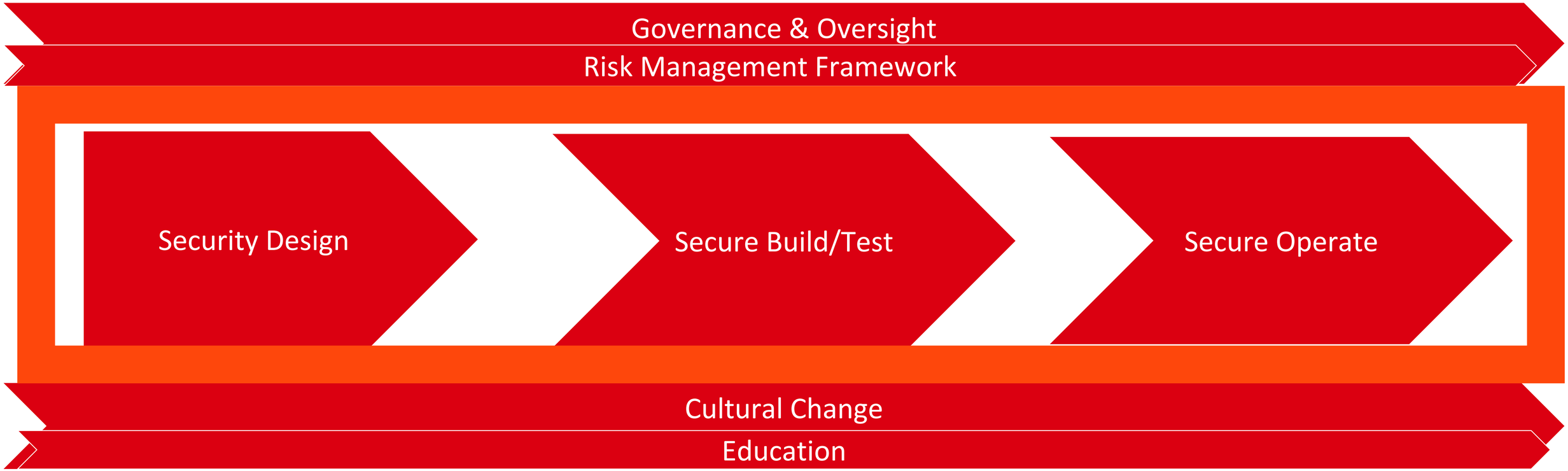
Vulnerability management
Risk management
Patching
Compensating controls activities

Vulnerability Mangment Framework

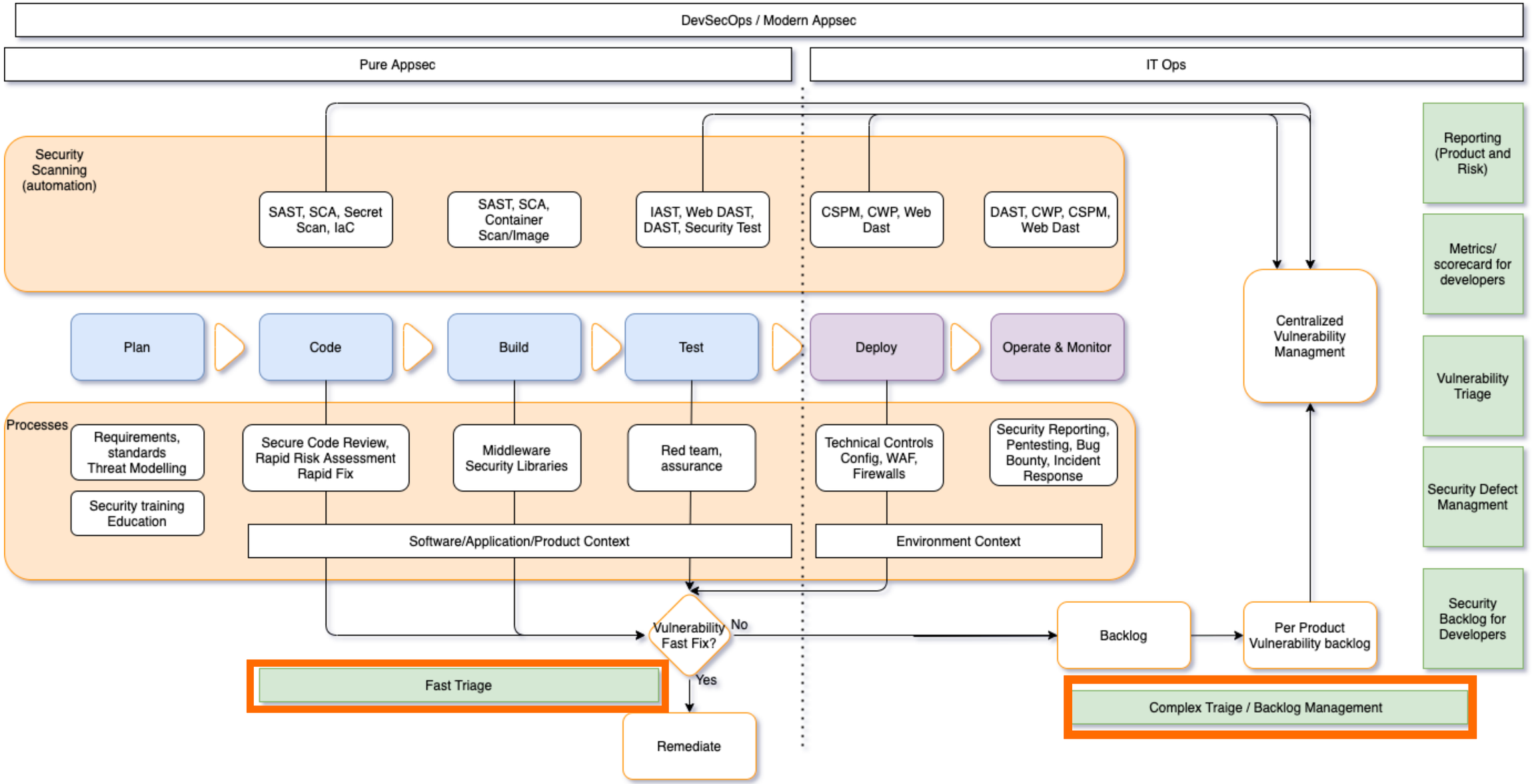
LEVEL	DETECTION	AGGREGATION/ ASSET MANAGMENT	PRIORITIZATION	ACTION	MEASUREMENT
M0	No Scan No Detection No Pentest	No Aggregation	No Prioritization	No action, ad-hoc reaction	No measurement No tracking
M1	Policy for Detection and scan Regular Pentest No SCA/ Library detection	Aggregate Vulnerabilities	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

WHY ARE WE HERE?
Modern Software Pipeline

Vulnerability Maturity Frameworks – Stages and focus



Modern Security Pipeline



PROCESS OF TRIAGE

SLOW DEFENDER

180-280 days

Average time to fix a vulnerability

FAST ATTACKER

3-15 days

Average time to exploit a new vulnerability

DISCOVER

PRIORITIZE

ASSESS & ACT

Measure

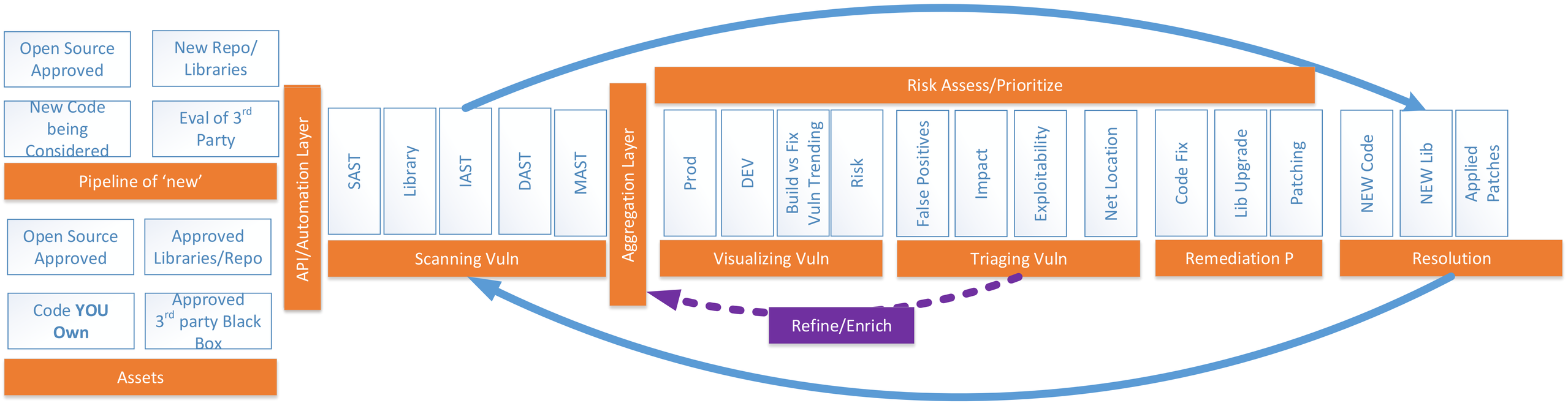
- Discover
- Scan
- Aggregate
- Triage
- Correlate
- Prioritize
- Find Team/ Route
- Chase/Follow-Up

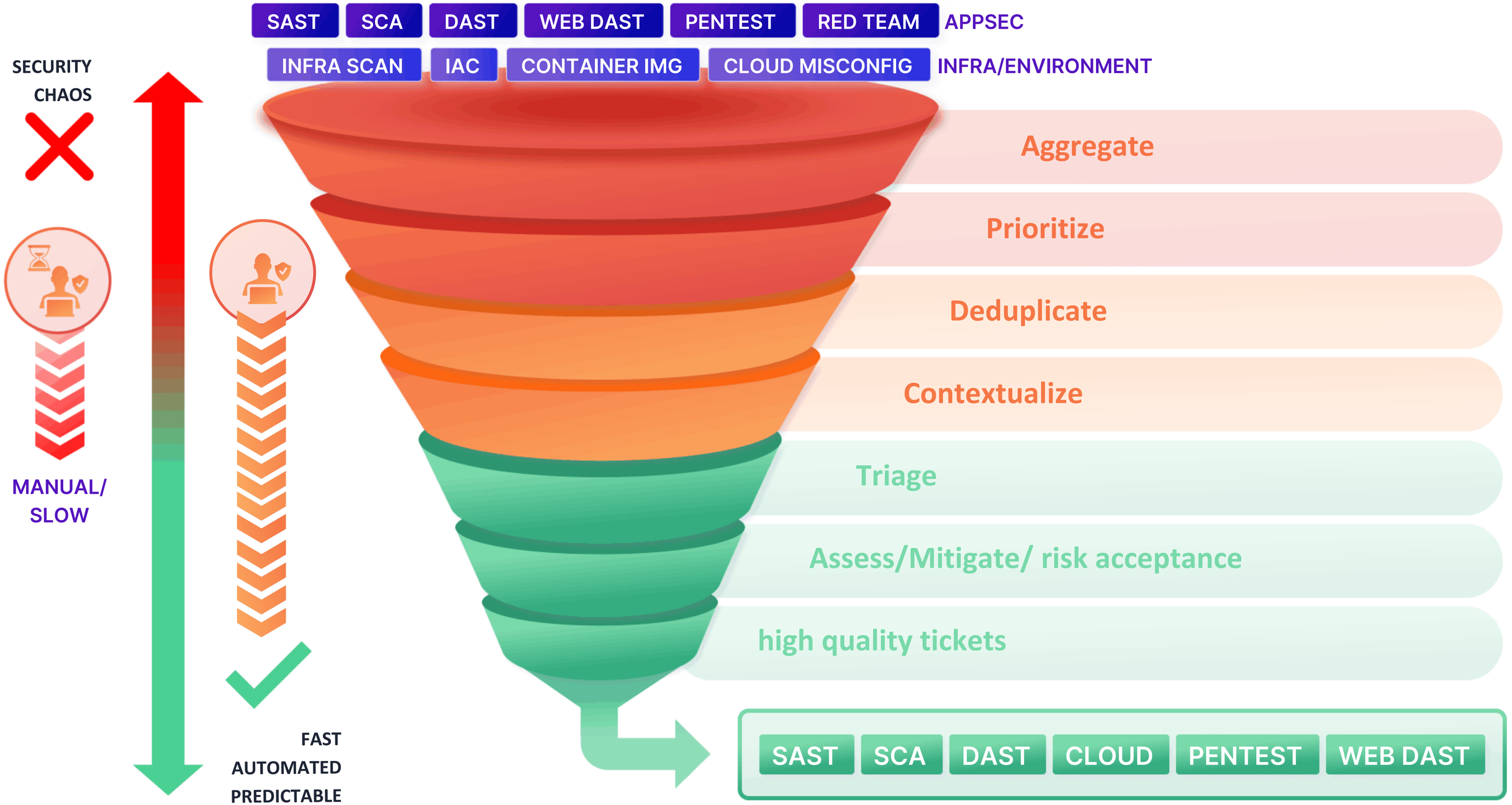
Exception Managment

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

- Discover
- Scan
- Prioritize
- Exploit
- Resolve

Vulnerability management Lifecycle -> Linear?

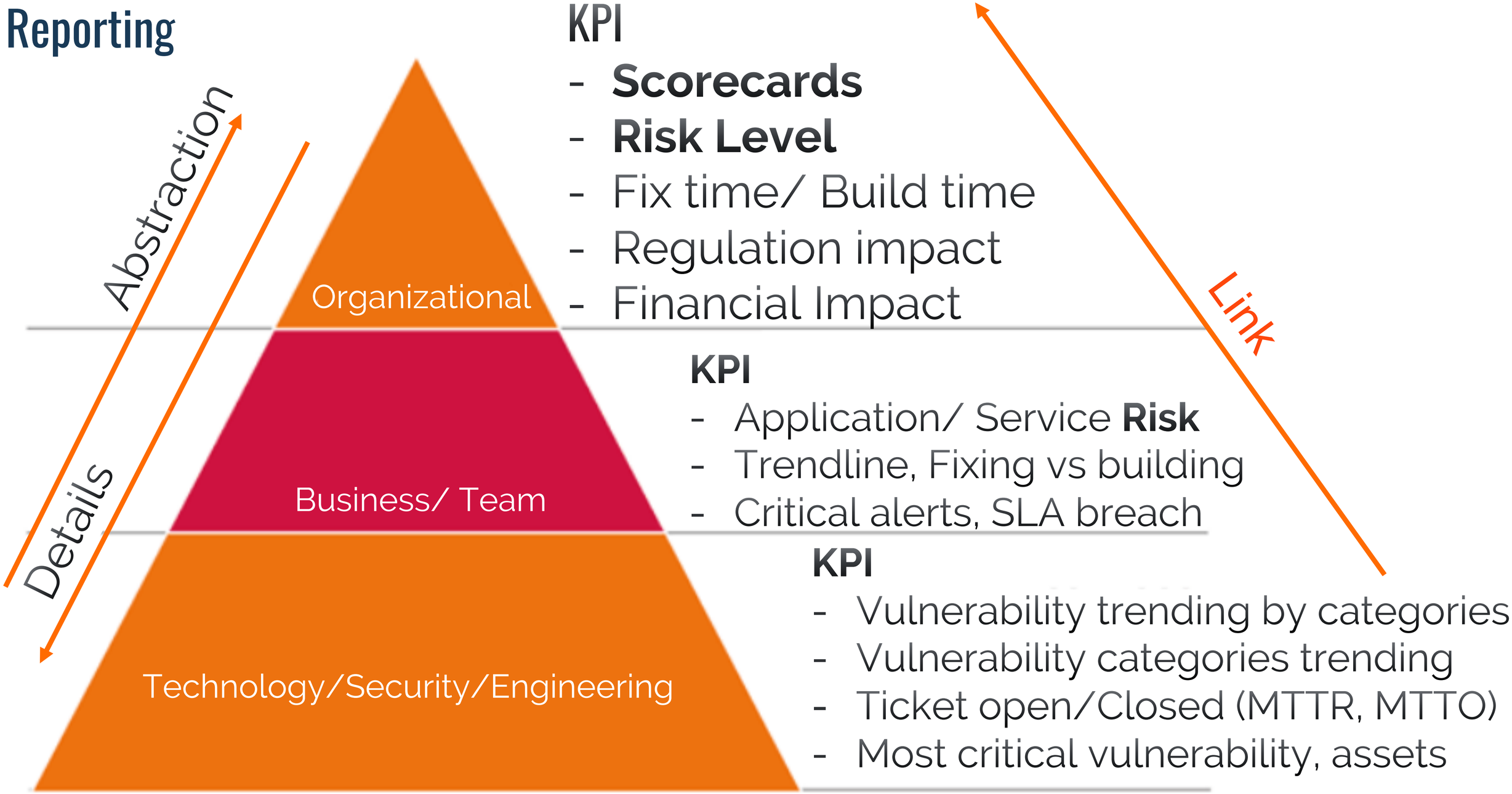




TO REPORT OR NOT TO REPORT

Reporting

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

Vulnerability management Framework

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

PRE ASSESSMENT

LEVEL	DETECTION	AGGREGATION/ ASSET MANAGMENT	PRIORITIZATION	ACTION	MEASUREMENT
M0	• No Scan • No Detection • No Pentest	• No Aggregation	• No Prioritization	• Fix Random	• No measurement • No tracking
M1	• Policy mandating scanning requirements / Secure SDLC • Regular Pentest / External Scan • No SCA/ Library detection	• Aggregate Vulnerabilities in central place	• Prioritization based on vulnerability severity	• Fix based on severity	• 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	• Number of vulnerabilities • SLA per criticality
M3	• Policy mandating scanning requirements / Secure SDLC • Regular Pen-test / External Scan • Automated Static code analysisInfra 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)	• SLA per criticality • SLA Risk based
M4	• Policy mandating scanning requirements / Secure SDLC • Regular Pen-test / External Scan • Automated Static code analysisInfra 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) • 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 burndown • SLA Risk based, • False Positive/Exception rate • Technology Insights • Security OKR • Security Insights • Build vs Fix stories • Localized insights (per business application)

POST

LEVEL	DETECTION	AGGREGATION/ ASSET MANAGMENT	PRIORITIZATION	ACTION	MEASUREMENT
M0	• No Scan • No Detection • No Pentest	• No Aggregation	• No Prioritization	• Fix Random	• No measurement • No tracking
M1	• Policy mandating scanning requirements / Secure SDLC • Regular Pentest / External Scan • No SCA/ Library detection	• Aggregate Vulnerabilities in central place	• Prioritization based on vulnerability severity	• Fix based on severity	• 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	• Number of vulnerabilities • SLA per criticality
M3	• Policy mandating scanning requirements / Secure SDLC • Regular Pen-test / External Scan • Automated Static code analysisInfra 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)	• SLA per criticality • SLA Risk based
M4	• Policy mandating scanning requirements / Secure SDLC • Regular Pen-test / External Scan • Automated Static code analysisInfra 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) • 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 burndown • SLA Risk based, • False Positive/Exception rate • Technology Insights • Security OKR • Security Insights • Build vs Fix stories • Localized insights (per business application)

Detection of issues

DETECTION > AGGREGATION/ DEDUPLICATION > PRIORITIZATION > ACTION > MEASUREMENT

M0	M1	M2	M3	M4	M5
No Scan No Detection No Pentest	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 / 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

Aggregation & Deduplication

DETECTION > AGGREGATION/ DEDUPLICATION > PRIORITIZATION > ACTION > MEASUREMENT

M0	M1	M2	M3	M4	M5
• No Aggregation	• Aggregate Vulnerabilities in entral place	• Aggregate vulnerabilities per business application • Aggregation of Assets • Deduplication - L0 - Manual	• Aggregate vulnerabilities per business application • Aggregation of Assets • Asset contextualization (business) • Deduplication L1 - Automated - (Assets Dedup, CVE Dedup)	• 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	• 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

DETECTION > AGGREGATION/ DEDUPLICATION > **PRIORITIZATION** > ACTION > MEASUREMENT

M0	M1	M2	M3	M4	M5
• No Prioritization	• Prioritization based on vulnerability severity	• Prioritization based on vulnerability severity • Prioritization based on SLA (severity)	• Prioritization based on vulnerability severity • Prioritization based on Risk/ Risk Based SLA • Prioritization based on Cyber threat intelligence	• Prioritization based on vulnerability severity • Prioritization with Risk/ Risk based SLA • Prioritization based on Cyber threat intel • Prioritization based on business contextual information	• 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,

Action / Routing

DETECTION > AGGREGATION/ DEDUPLICATION > PRIORITIZATION > **ACTION** > MEASUREMENT

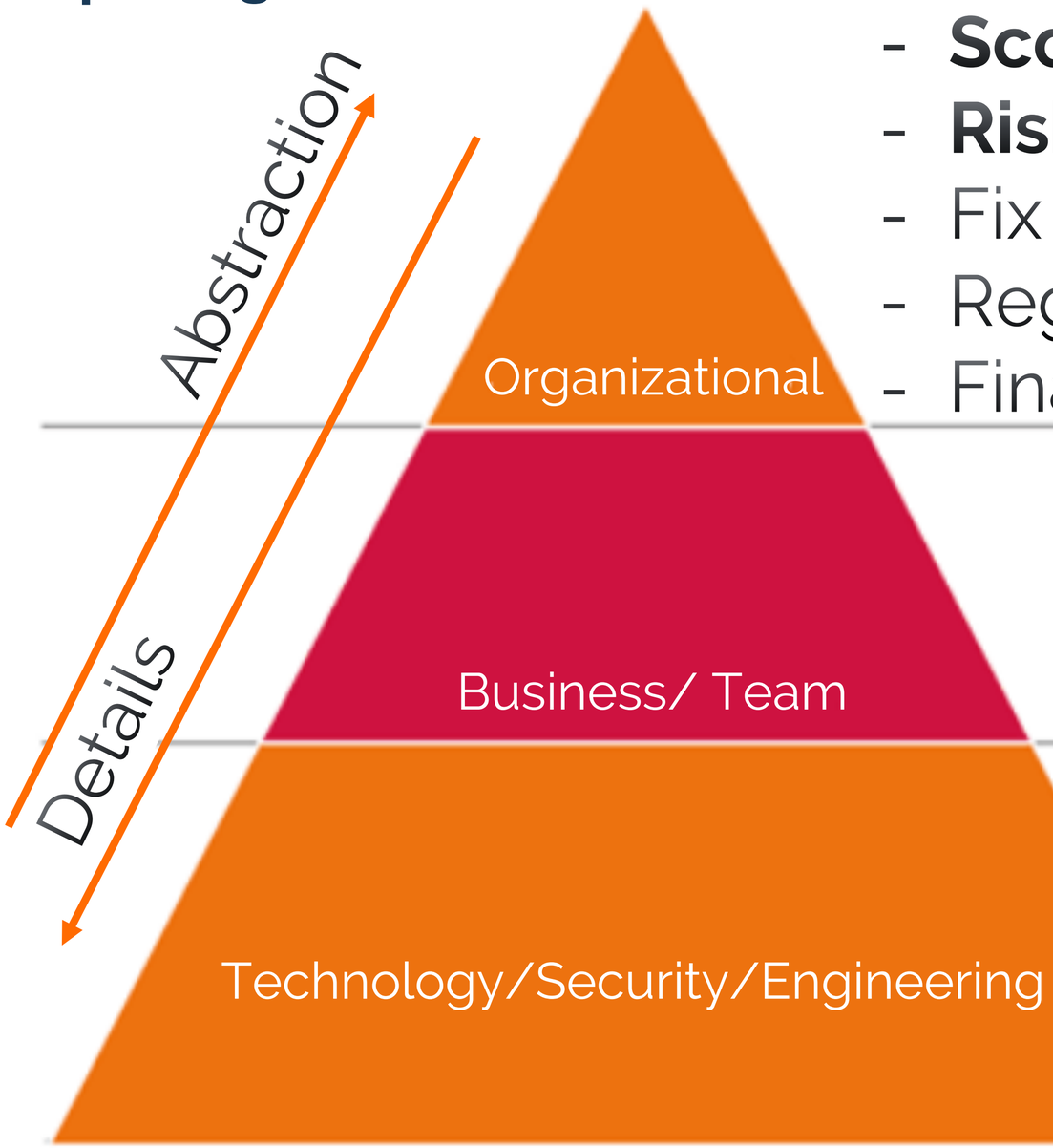
M0	M1	M2	M3	M4	M5
• No Action	• Reactive and Regular review of vulnerability actions	• Regular Review of vulnerability actions • Regular Burn down of Vulnerabilities by SLA	• Regular review of Backlog • Regular Burn down of top vulnerabilities in the backlog	• Regular review of Backlog • Regular Burn 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	• 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

Measuring Progress

DETECTION > AGGREGATION/ DEDUPLICATION > PRIORITIZATION > ACTION > MEASUREMENT

M0	M1	M2	M3	M4	M5
• No measurement No tracking	• Number of vulnerabilities/ Vulnerability Severity	• Number of vulnerabilities • SLA per criticality	• SLA per criticality • SLA Risk based	• SLA per criticality • SLA Risk based • Mean time to resolution • Security balanceFalse Positive/Exception rateSecurity 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)

Reporting



KPI

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

Link

KPI

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

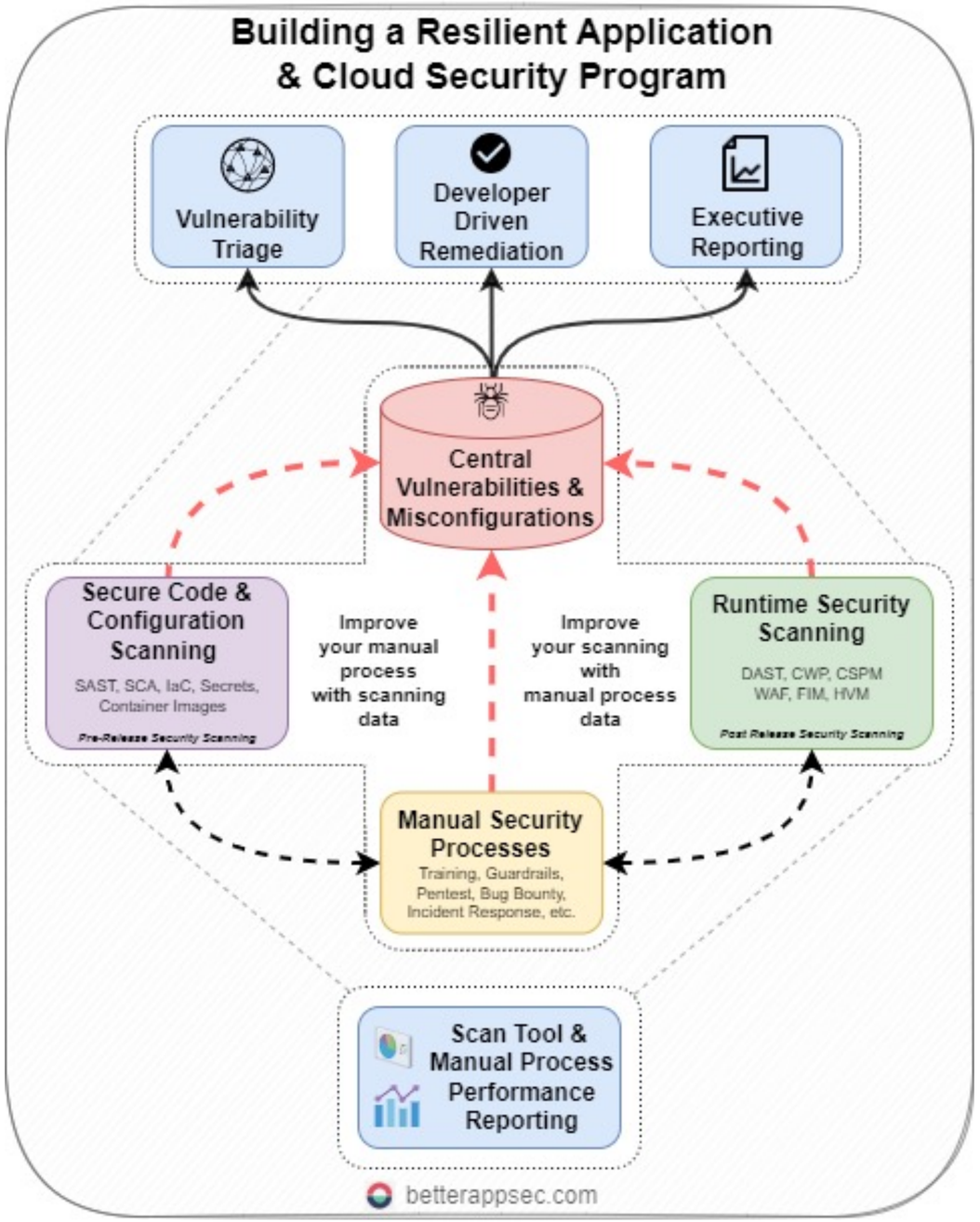
KPI

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

Conclusion & Recap

CENTRALIZE RESULTS/ MEASURE LEFT AND RIGHT

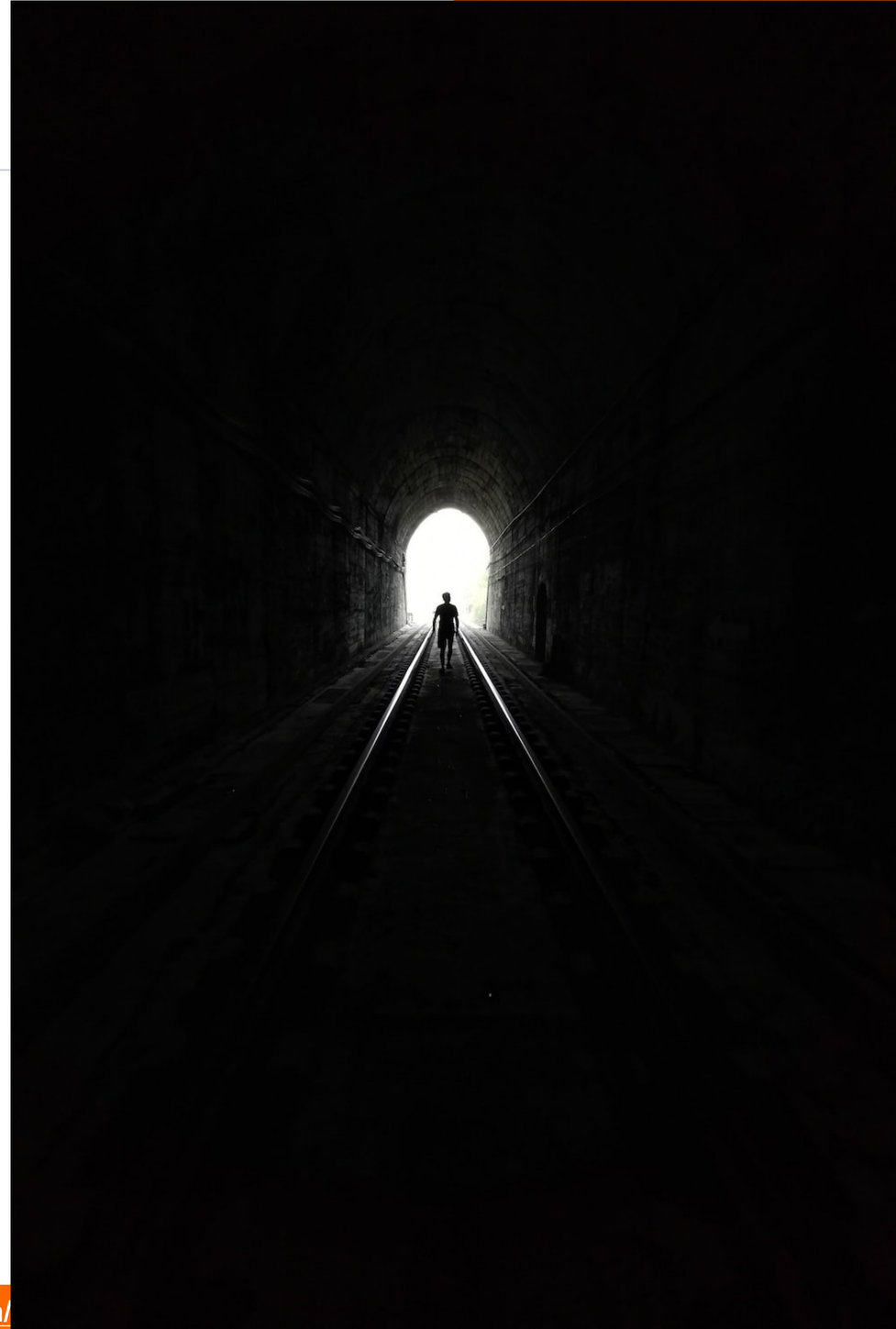
Security Scanning
- **Left (code pre deploy)**
- **Right, Post build**
- **Manual Ops**



Light at the end of the tunnel

There is a light at the end of the tunnel

- Identify issue
- Decide Maturity level and setup process, procedure tooling
- Collaborate & sit down with teams
- Talk with business – shift up
- Talks with the dev – shift left
- Vulnerability management Framework



ACT NOW ON RISK & FIX VULNERABILITIES

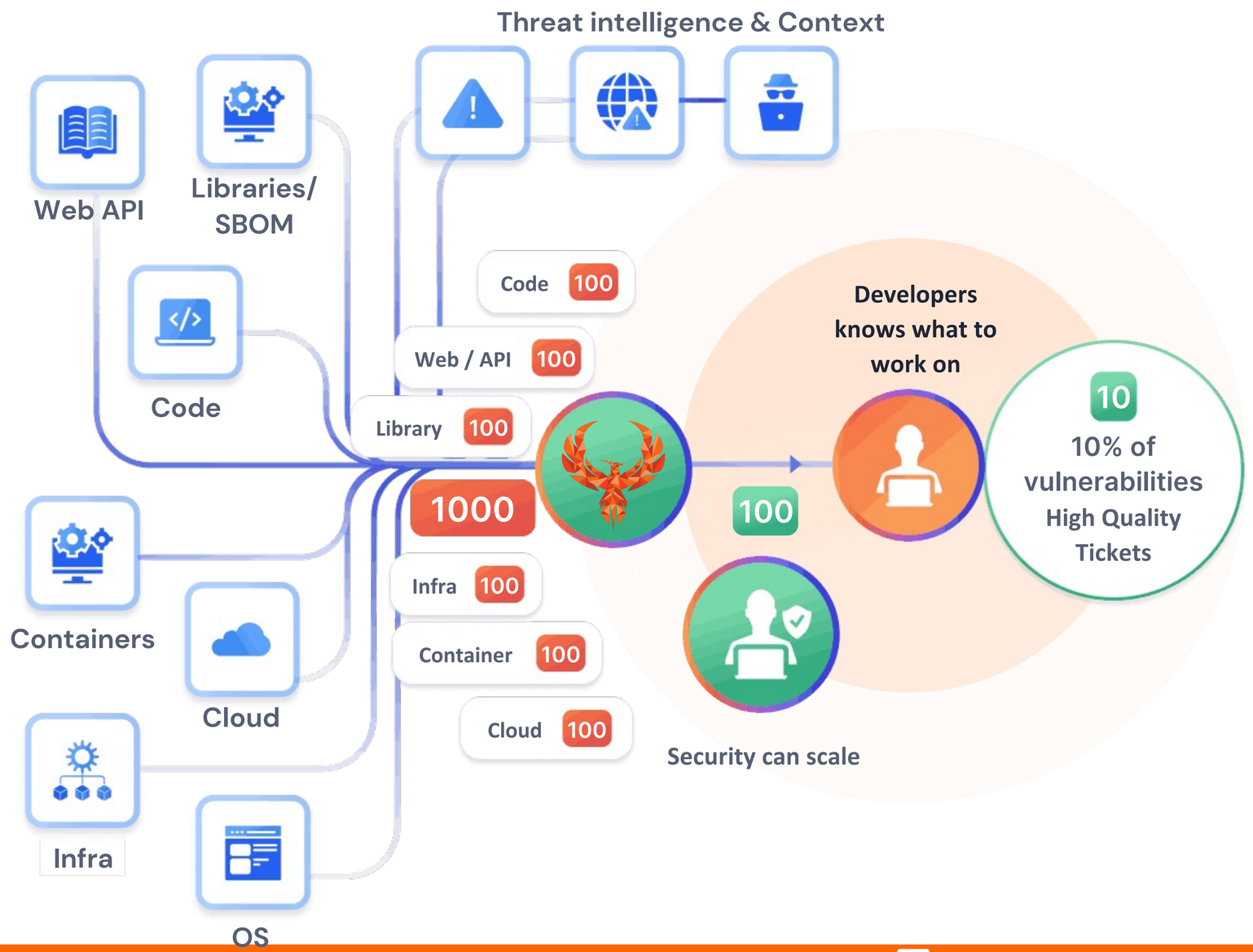
PHOENIX

Posture Management
For Cloud & Application Security

Vulnerability management framework material

https://phoenix.security/vulnerability-management-framework/

Phoenix Security – Narrative on security



AGGREGATE & CONTEXTUALISE VULNERABILITIES

REMOVE MANUAL ACTIONS, TRIAGE AUTOMATICALLY

REMOVE INEFFICIENCIES PRIORITIZE ACTIONS NO BURNOUT

OWASP License -

We love OWASP Community Edition Available

APPSECPHOENIX

APPSECPHOENIX

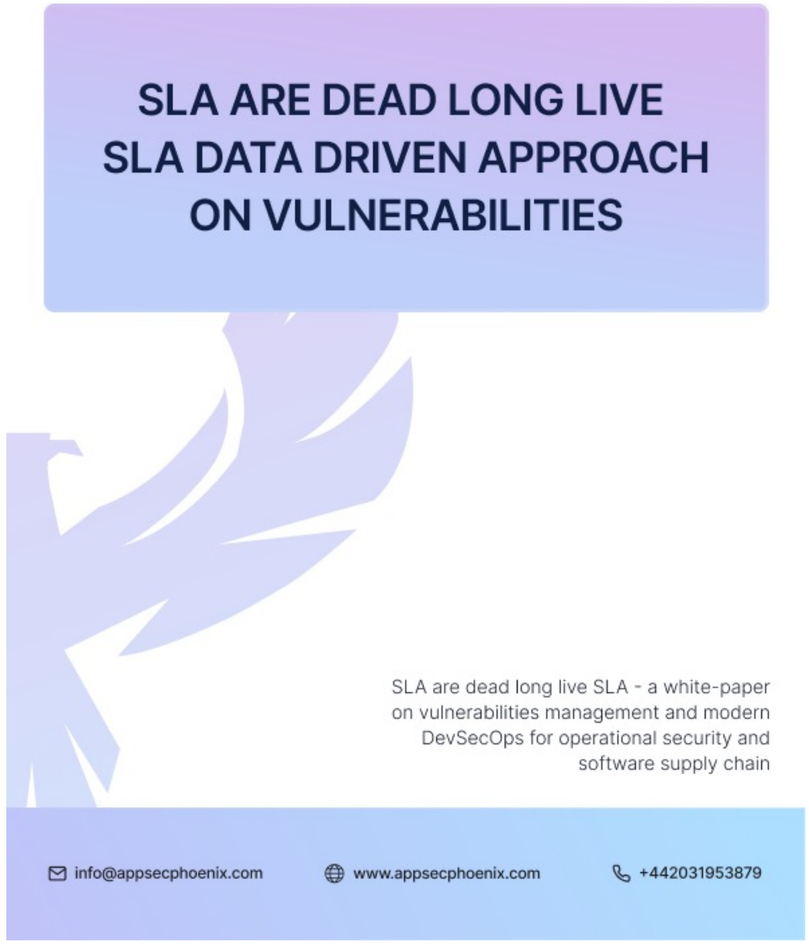
1000 Users

350 Organizations

SMART APPLICATION SECURITY

New Book on metrics that matters

PHOENIX SECURITY



Q&A

Thank you

Cyber Security & Cloud Podcast

By Francesco Cipollone

#CSCP

www.cybercloudpodcast.com

@podcast_cyber

@FrankSEC42

www.cybercloudpodcast.com

Sponsored By

APPSEC PHOENIX

SMART SECURITY

APPSEC PHOENIX

Phoenix Security

Removing Manual work to automate, scale more 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$,
Dev average daily rate 300$