The Security Phoenix raises from DEV-OPS ashes

A Modern Approach on DevSecOps Focused on People

DevOPS.com webinars - White Source Webinars

@FrankSEC42

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

https://uk.linkedin.com/in/fracipo

NSC42

Agenda

- About the Francesco
- Context
  - Security Phoenix – Maturity matrix
  - Appsec & Breaches in numbers
  - Visibility Problem
  - The cake and traceability problem
- The Security Phoenix – Appsec Program
  - Security Phoenix Program – People & Trust + Verify
  - Security Phoenix – Scanners Triage and Visualizers
  - Security Phoenix – Maturity Matrix & Education
- Conclusions
- Q&A

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

About Francesco

WhiteSource

Francesco Cipollone

Founder – NSC42 LTD

CSA cloud security alliance UK & IRELAND

(ISC)² OFFICIAL CHAPTER LONDON

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

I've been helping organizations define and implement cybersecurity strategies and protect their organizations against cybersecurity attacks

HSBC Nationwide UNITED NATIONS BT vodafone ELEXON CAPITA Asset Services

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

Security is everybody's job

We need to make security cool and frictionless

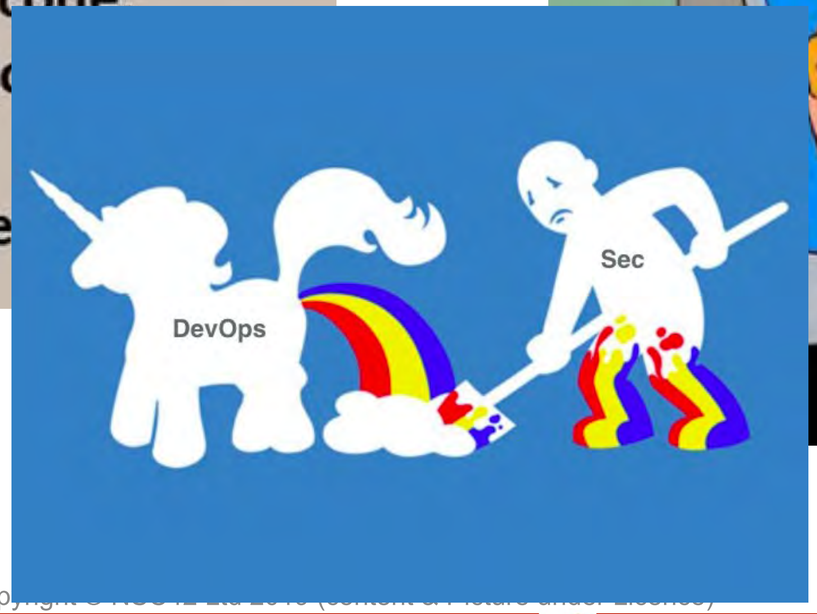
Copyright © NSC42 Ltd 2019

What do I usually talk about?

WhiteSource

Appsec

Cloud Sec



Copyright NSC42Ltd 2020

WhiteSource

What kind of animal is the DEV-SEC-OPS?

Integrate security into the OPS team (and add a spark of RISK)

DEV-OPS+
SEC

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

The Problem Landscape: Numbers behind the breaches

Why do we worry about security?

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

WhiteSource

Why fixing Security Vulnerabilities is everybody's job?

…because we all get affected by it

2009/2010
- Microsoft
- Heartland
- US Military
- Aol
- TJMax

2012
- Sony PSN
- NHS
- Betfair
- Steam

2012
- Dropbox
- Lastfm
- Blizzard

2013
- Yahoo(orignal)
- US Retailers
- Adobe
- UbiSoft
- Court Ventures

2014
- JP Morgan
- Home Depo
- Ebay

2015
- Deep Root
- IRS
- Anthem

2016
- Linkedin
- Friend Finder
- Dailymotion
- Mossack Fonseca

2017
- Equifax
- Myspace
- Twitter
- Yahoo

2018
- Marriot
- Twitter
- MyHeritage
- Uber
- Quora..

2019/2020
- Capital One
- British Airways
- Travelex
- Fortnite
- WhatsApp/ Instagram
- Blackrock
- Facebook x2
- Docker Hub
- AMC

2020

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

Major Breaches

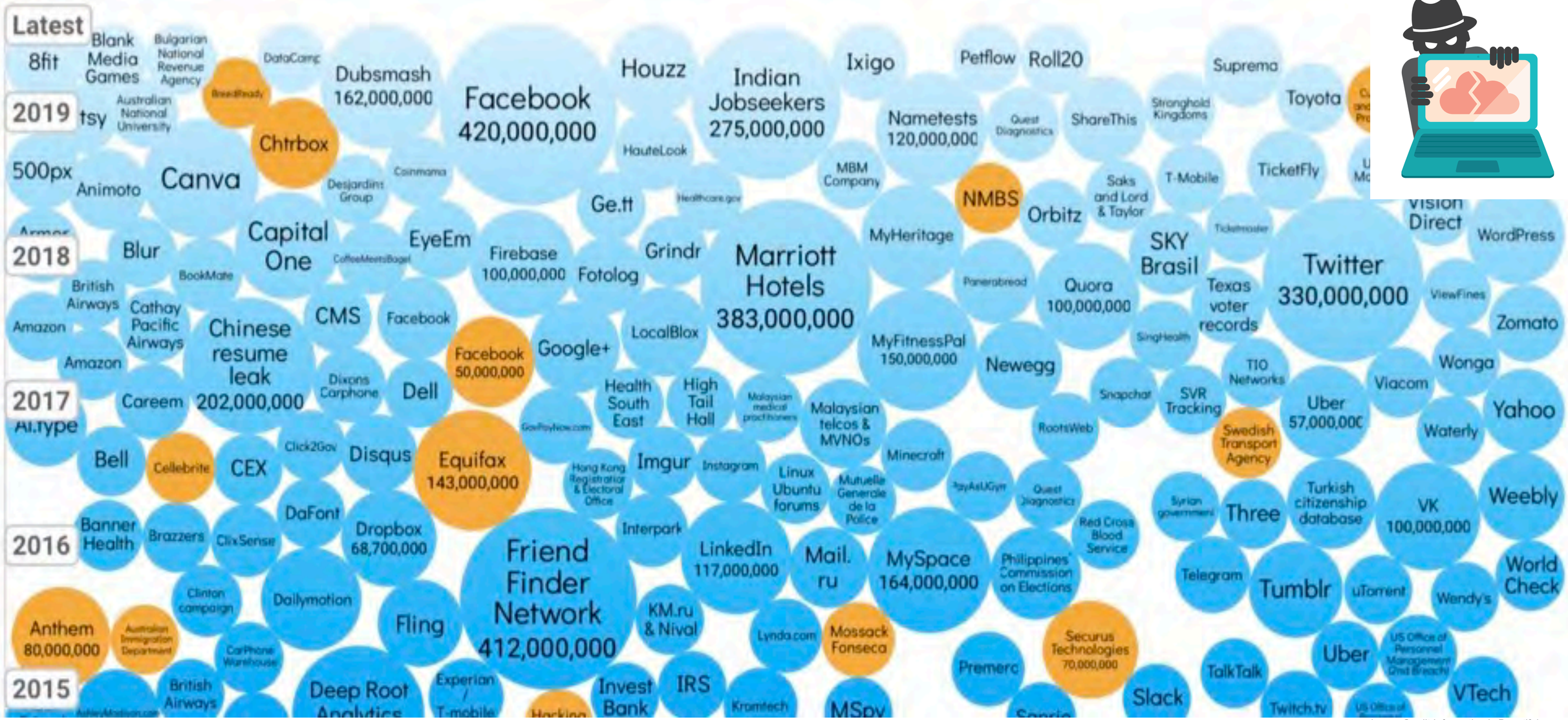


Image Credit Information is Beautiful

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

TOP 5 Security Breaches

WhiteSource

1

Capital One (2019)

Misconfiguration of WAF (web application Firewalls) – 106 mil records

2

Marriott (2018/2020)

Second time access breach after 2018 hack

3

Nintendo (April 2020)

Credential stuffing from previous hack

4

British Airways (Sept 2018)

Injection of code in a library

5

Microsoft & Facebook (2018-19)

Data found in unprotected DB (public access) + Misuse of API (facebook)

Common Mistakes

The common theme around all those breaches are

1. **Misconfiguration**
2. **Open Source Libraries Injection/Vulnerabilities**
3. **Common Vulnerabilities (OWASP Top 10)**
4. **Public Storage (data left unauthenticated)**
5. **Easy to guess credentials (cred Stuffing) - Collection X anyone?**
6. **No MFA on critical accounts**
7. **Unchecked Open source software**
8. **Break of logic (API abuse)**

Scale of Equifax breach

The Equifax data breach was one of the largest in history. The company announced the data breach in September 2017, eventually reporting that 147 million consumers were affected. Hackers were able to get access to a multitude of consumer private information, including names, Social Security numbers, dates of birth, credit card numbers and even driver's license numbers.

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

Malicious Actors

WhiteSource

Well Known/Hacktivism

Anonymous, Lizard Squad, LulzSec, Chaos Comp Club, Syrian Elect Army

Financially motivated

Gold Southfield- ReEvil, Magecart, Lazarus group …

Less visible more dangerous

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

Breaches in Number - appsec

WhiteSource

Adversaries don't need many vulnerabilities - ONE is enough.

Is your business equipped with the right tools to react fast enough?

Av Cost of data Breach

3.03 m

Every

36 minutes

A new security vulnerability is identified

N. Of Vuln per year

1400 vuln

As disclosed vulnerabilities

It takes

150-180 days

To fix a vulnerability

It takes

3-15 days

To exploit a vulnerability

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

Cost of Security

Adversaries don't need many misconfiguration ONE is all it takes.

Is your business equipped with the right tool and trusted partner to address it?

Total cost of breaches

5 trillion $ / 4 trillion GBP

Every min

62K record disclosed

Record per minute disclosed

N. Of Vuln records

33 billion

Disclosed records over 1 year

Data breaches

80% due to misconfiguration

Cloud misconfiguration is dominat

Av. Cost per record

150$ per record

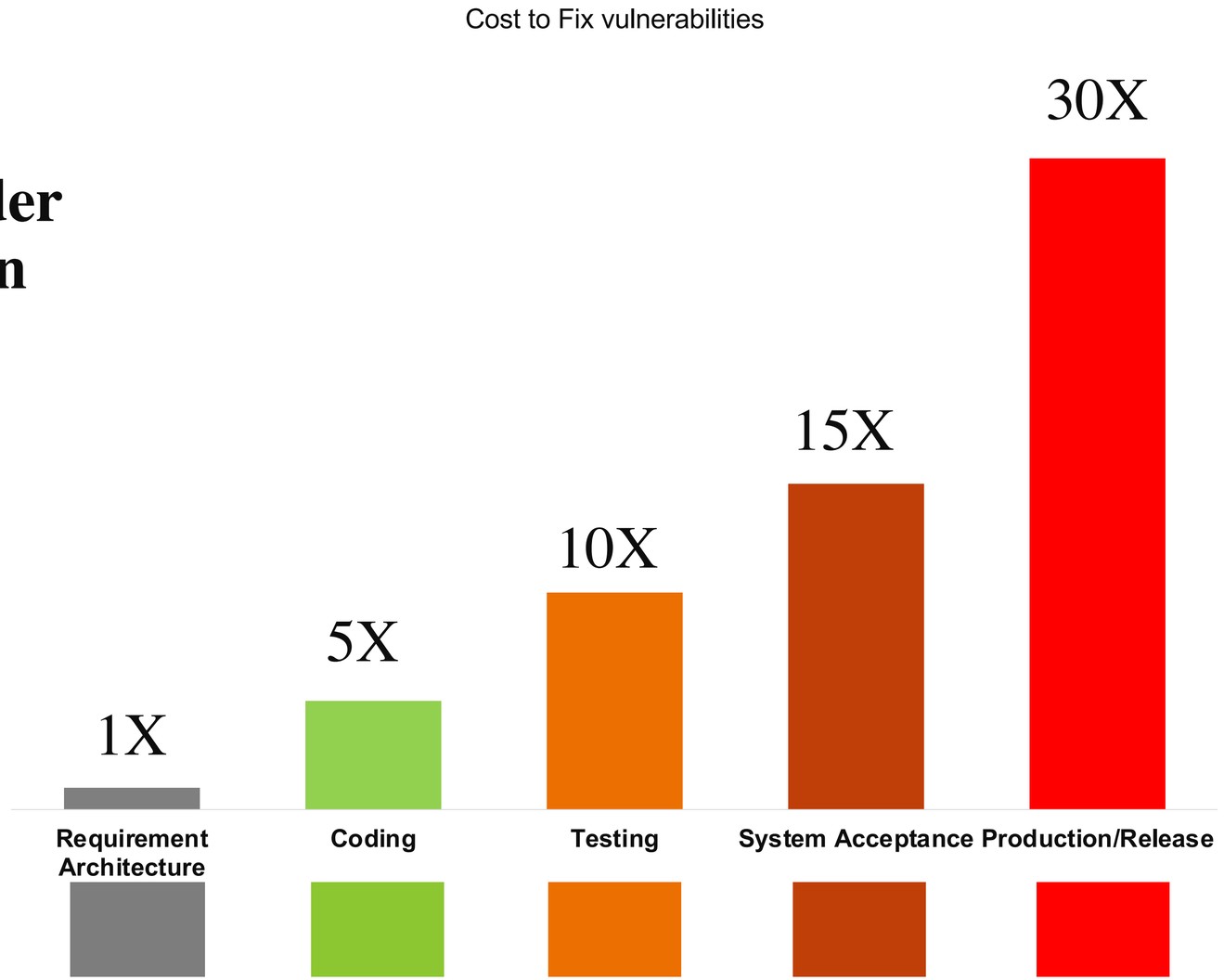
Average cost per loss record

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

Cost to fix

Fixing vulnerabilities gets harder and harder the more they are in production

The earlier they are identified and fixed the less costly/time consuming the fix becomes



Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

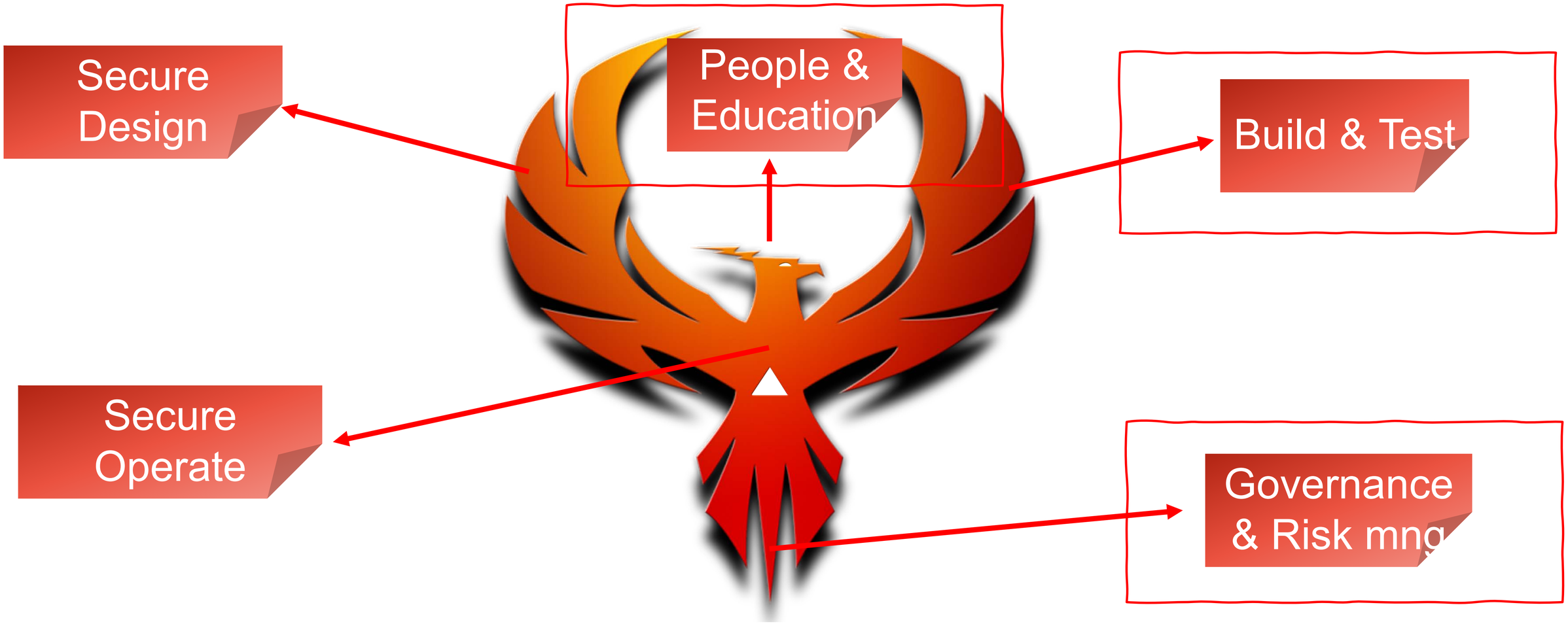
The Security Phoenix

Appsec Program based on Data and People

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

WhiteSource

What Are the core pillars of Security Phoenix



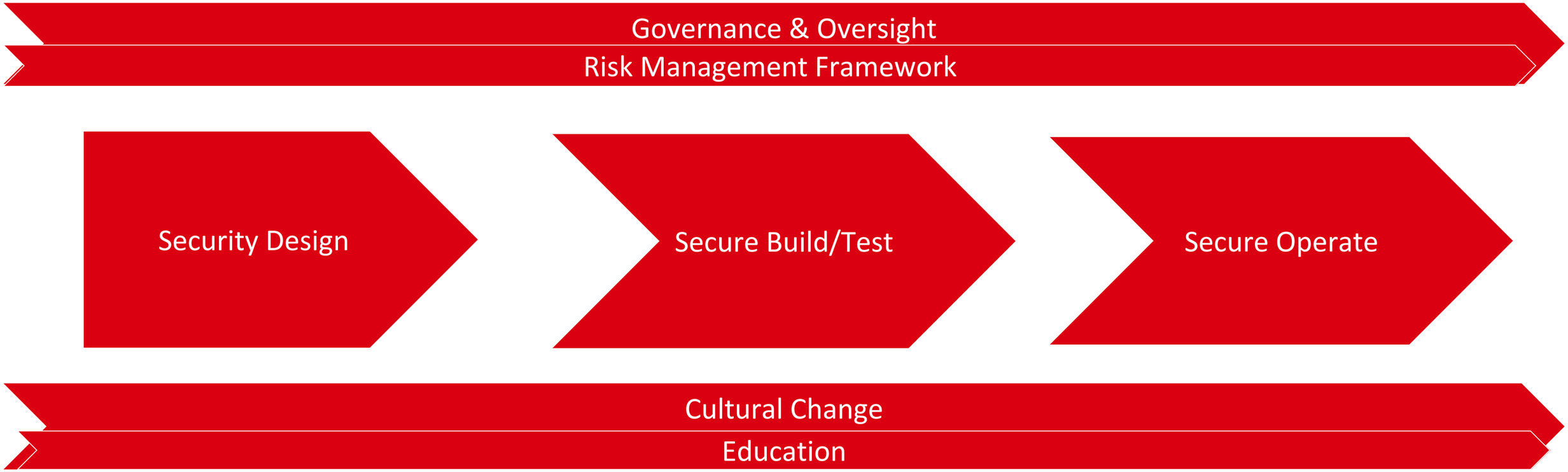
Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

WhiteSource

How do we get better and measure it?

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

Importance of Maturity Models/Matrix - NSAMM



Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

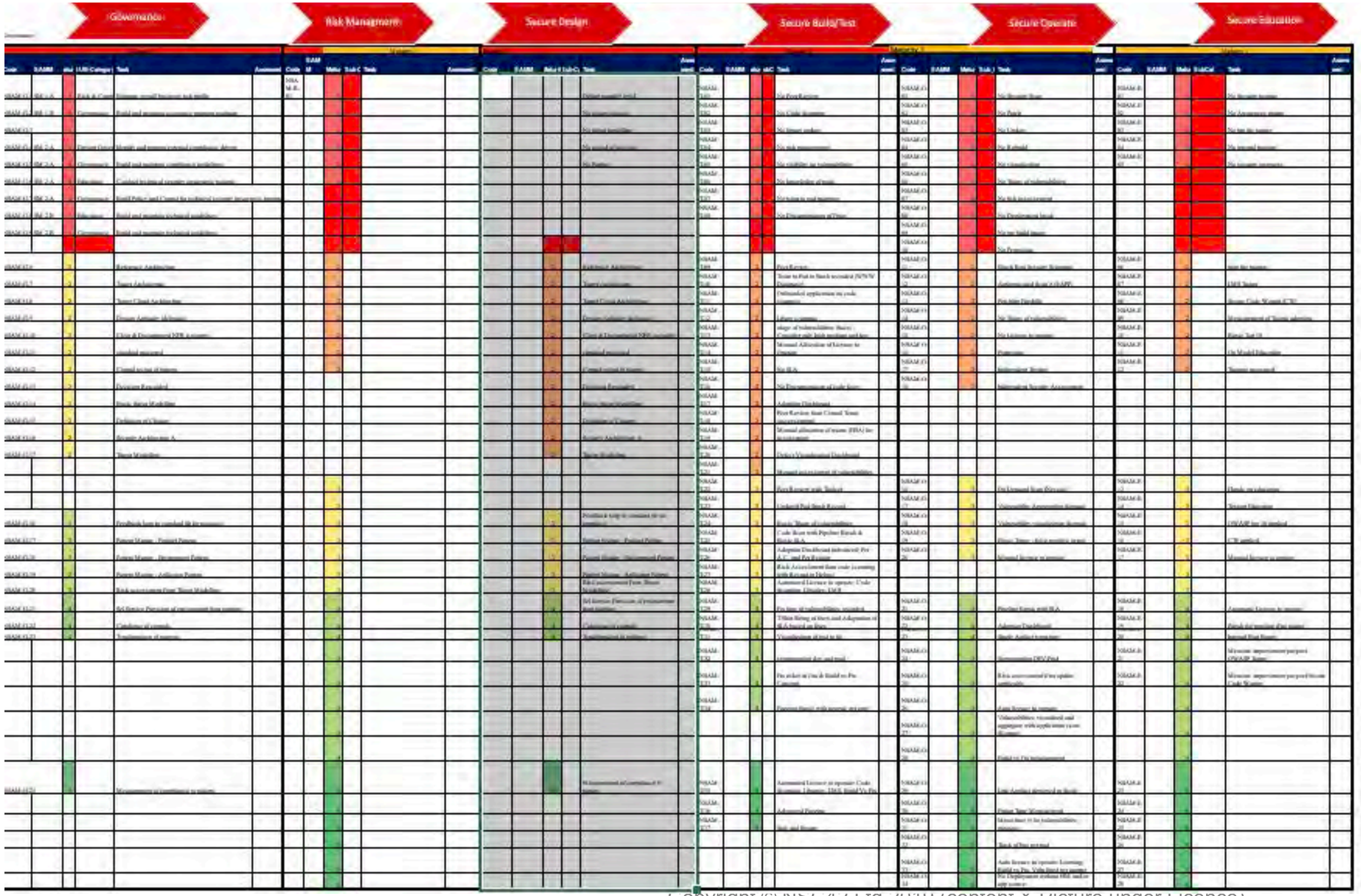
Importance of Maturity Models/Matrix - NSAMM

AS-IS					
Time	2019				
	Level 1	Level 2	Level 3	Level 4	Level 5
	Intial	Managed	Defined	Quantitatively Ma	Optimized
Security Design	AS-IS				
Security Design Governance	AS-IS				
Security Build & Test	AS-IS				
Security Operate		AS-IS			
Security Education		AS-IS			
Application Security Risk Management		AS-IS			

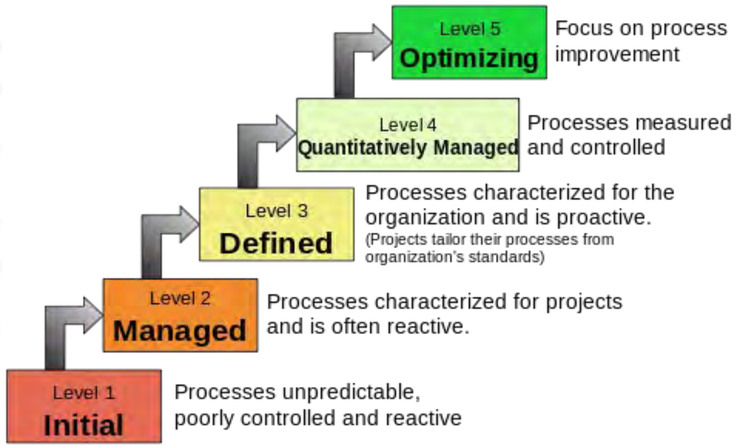
TO-BE					
Time	2020				
	Level 1	Level 2	Level 3	Level 4	Level 5
	Intial	Managed	Defined	Quantitatively Ma	Optimized
Security Design		TO-BE			
Security Design Governance		TO-BE			
Security Build & Test		TO-BE			
Security Operate		TO-BE			
Security Education		TO-BE			
Application Security Risk Management		TO-BE			

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

Importance of Maturity Models/Matrix - NSAMM



Characteristics of the Maturity levels



Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

Importance of Maturity Models/Matrix - NSAMM

DEV Security

Production Security

Overall Maturity

	Level 1	Level 2	Level 3	Level 4	Level 5
	Intial	Managed	Defined	Quantitatively Managed	Optimized
Security Design	AS-IS->TO-BE				
Security Design Governance	AS-IS	TO-BE			
Security Build & Test	AS-IS	TO-BE			
Security Operate		AS-IS-> TO-BE			
Appsec Security Education	AS-IS	TO-BE			
Application Security Risk Management	AS-IS	TO-BE			

Maturity Steps

Maturity	Task	How much
1	No Peer Review	
1	No Code Scanning	
1	No library update	
1	No risk management	
1	No visibility on vulnerabilities	
1	No knowledge of pods	
1	No team to pod mapping	
1	No Documentation of Fixes	
2	Peer Revew	
2	Team to Pod to Stash recorded	
2	Onboarded application on code scanners	
2	Libray scanning	
2	triage of vulnerabilities (base) - Consider only high medium and low	
2	Manual Evaluation of team and Allocation of Licence to Operate	
2	No SLA	
2	No Documentaiton	
2	Adoption Dashboard	
3	Peer Review with Toolset	
3	Updated Teams and asset register	
3	Basic Triage of vulnerabilities	
3	**Code Scan with Pipeline Break & Basic SLA**	
3	Adoption Dashboard (advanced) Per A.C. and Per Region	
3	Risk Assessment from code scanning with record in Risk management Register	
3	Automated Licence to operate: Code Scanning, Libraries, Internal Training	
4	Fix time of vulnerabilities recorded	
4	T-Shirt Sizing of fixes and Adaptation of SLA based on fixes	
4	Visualization of pod to fix	
4	segmentation dev and prod	
4	Fix ticket in Jira & Build vs Fix Concept	
4	Fuzzing (basic with generic per app)	
5	Automated Licence to operate: Code Scanning, Libraries, Internal Training, Build Vs Fix	
5	Automated Fuzzing & Library of tests	

KCI

			Reporting Frequency
	KCI Matrutiy	Build/Test	
Prereq ->	0	Who is working on which repository	Monthly
	1	Team On-boarded on scanners (per pod)	Monthly
	1	Code Scanning Frequency per project (min 1 per week)	Monthly
	1	Dashboard for Scanners created	Monthly
	2	Number of vulnerabilities ticket recorded	Weekly
	2	Dashboard for vulnerabilities - Onboarded Projects	Weekly
	2	Vulnerability Fixed (quarter)	Monthly/ Quarterly Checks
	3	Project vulnerabilities integrated in Vulnerability management programme	Monthly
	3	Projects breaching the Build vs Fix target	Monthly/ Quarter Checks
	4	Fixes per thematic in SLA	Monthly
	4	SLA for Fixes (breached/achieved)	Monthly
	4	Team Achieving Licence to operate and Out of the licence	Monthly
	5	Build vs fix	Monthly
	5	Licence to operate	Monthly

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

The Visibility Problem

From Dev to prod and cakes

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

Understanding the room you walk in – Asset Register

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

To understand shine a light

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

Better to have full visibility

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

The Problem Traceability Problem

The software security cake

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

So how we do it? Easy as baking a cake

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

Road to Production: the cake analogy

Design

The Objective of the various areas are

- **Ingredients**
- **Recipe**
- **Stock List (asset Register)**

Security Design

Act as Health Inspector

- **Verify Ingredients are not mouldy**
- **Verify Recipe does not contain poison**
- **Stock List (asset Register) –** verify the component used in the cake are genuine

Build/Test

The Objective of the various areas are

- **Combine ingredients (libraries+Code)**
- **Bake the cake**
- **Test the cake**

Security Build & Test

Act as Health Inspector

- **That the cake is made up of genuine ingredients (from asset register)**
- **Test the cake for mould**

Operate

The Objective of the various areas are

- **Sell The cake**
- **Restock the cake on the shelf**

Secure Operate

Act as Health Inspector

- **Verify Cake on the shop are made of genuine ingredients (from asset register)**
- **Verify expiry data of Cake**
- **Test the cake for mould**

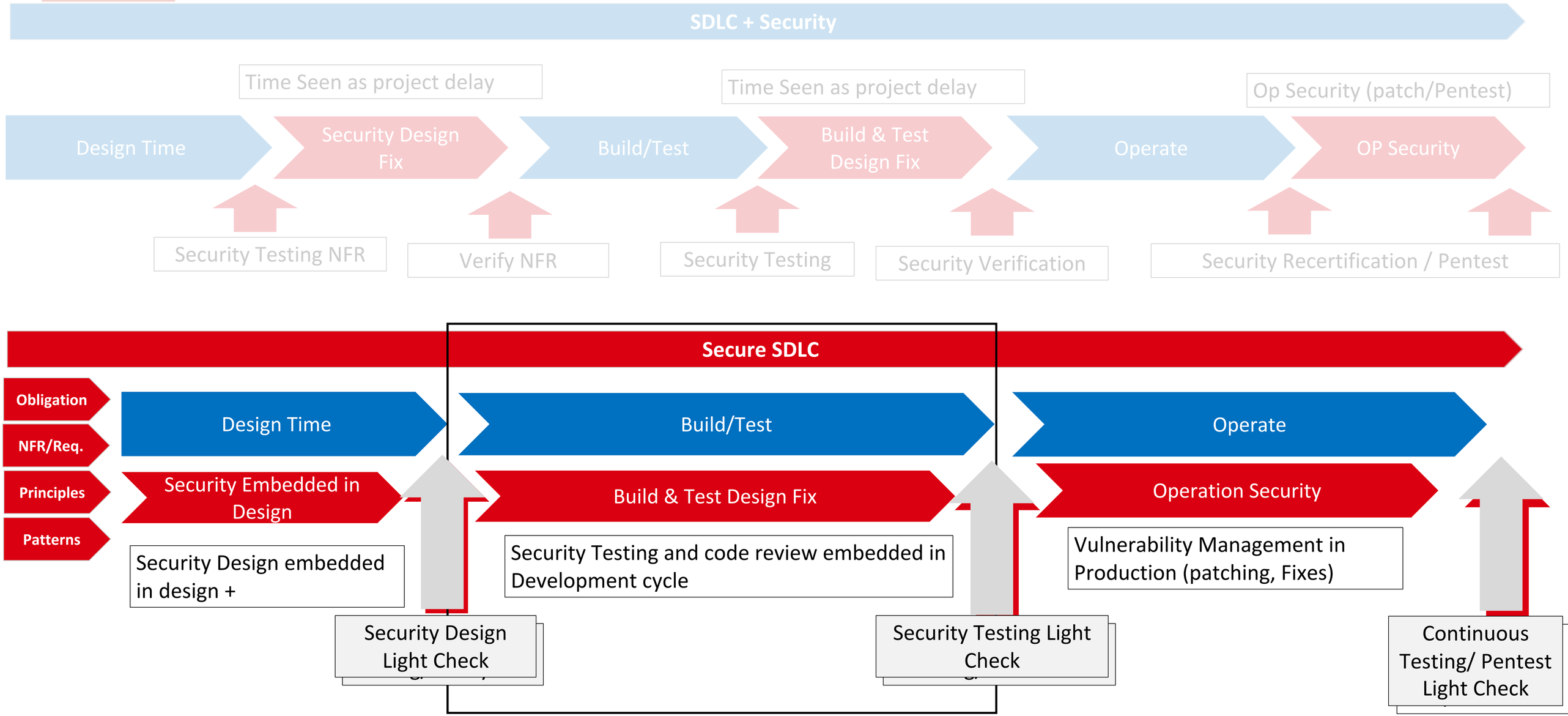
Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

The Appsec Lifecycle & Shift Left

The Software Asset Register

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

Shift Left - Meaning

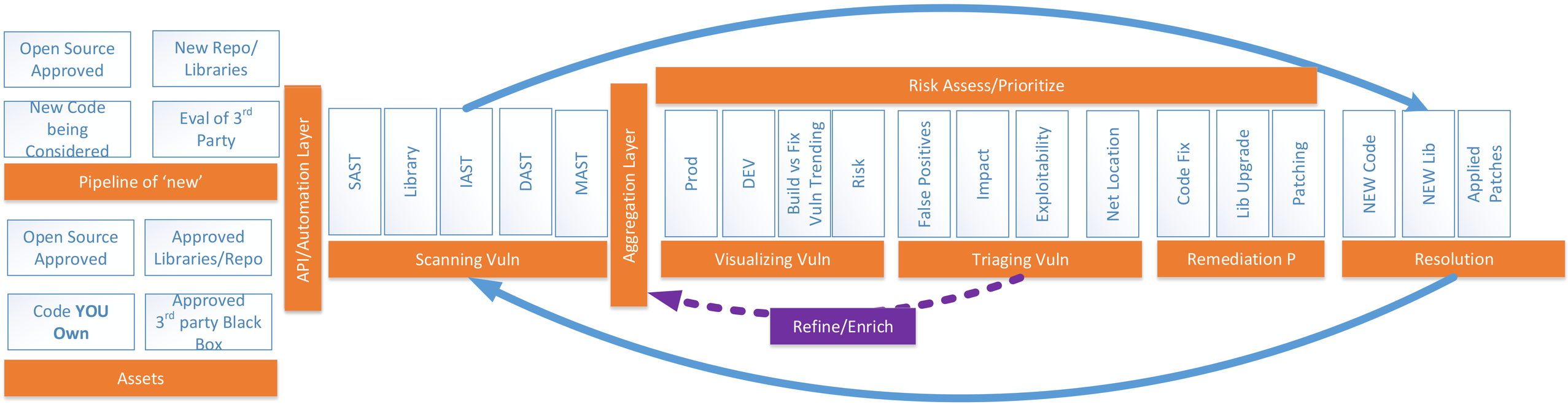


Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

Lifecycle Explored

DEV Security

Production Security



Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

Solving Visibility and Traceability Problem

Vulnerability management

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

Vulnerability management Definition

WhiteSource

"**Vulnerabilities** can be discovered with a vulnerability scanner, which analyses a code or system system in search of known vulnerabilities, such as code defect, insecure open source libraries, insecure software configurations, unpatched systems"

Vulnerability Assessment (VA) is not a scan, it is a one-time project with a defined start and end date.

Vulnerability Management (VM) is an ongoing process

Unlike a vulnerability assessment, a comprehensive vulnerability management program doesn't have a defined start and end date but is a continuous process that ideally helps organizations better manage their vulnerabilities in the long run.

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

Vulnerability management Lifecycle

WhiteSource

Software Asset Register
Scan Code/Infra/network

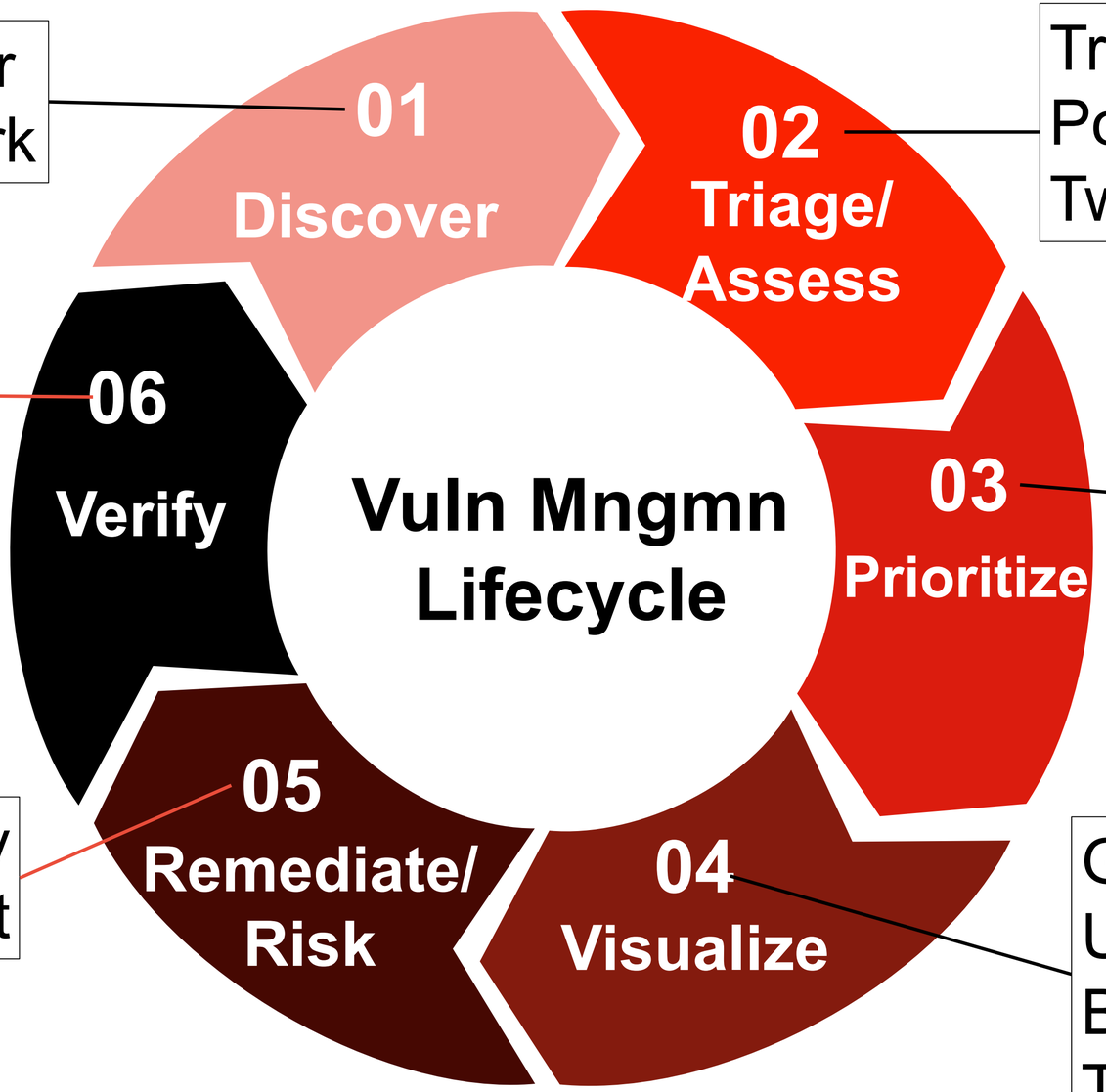
Triage & identify False Positives
Tweak Scan Profiles

Test implemented Fix

Prioritize vuln
(Start Easy)
Network Location
Exploitability
…

Fix Code and redeploy in test

Graph –
Up/down trending of prj
Build vs FIX
Time to Fix



Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

Fixing Vulnerability the ABC...D

WhiteSource

Outcome

Asset Register for	A - IDentify (Software Asset Register)		
	Software you build (repositories)	Software You buy	Trace Completeness across all the application you have
Vulnerability Data Lake	B – Detect (Scan Code)		
	Select Team Leads and identify security champions	Get security Scanners (SAST/DAST) Onboard and teach how to triage	Create a Vulnerability Data lake (results of the vulnerabilities)
KPI Reporting & Dashboard	C – Visualize Vulnerabilities (Display)		
	Reporting Dashboards (based on the maturity & KPI)	Link the trending to Build vs FIX, Vuln trending,	
Prioritizing & Vulnerability Reduction	D – Respond/recover (Fix Vulnerability)		
	7 – Schedule Vuln Fixes (Jira)	7 – Fix Vuln & measure (quarterly)	

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

The Traceability & People

Visualization & Accountability without finger pointing

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

What do you get out of Security Phoenix?

WhiteSource

1. Visualize and Fix Vulnerability at scale and pace (DEV & Ops)

2. Trust the Product team but keep them accountable: Trust & Verify & License to Operate

3. Maturity & Recap

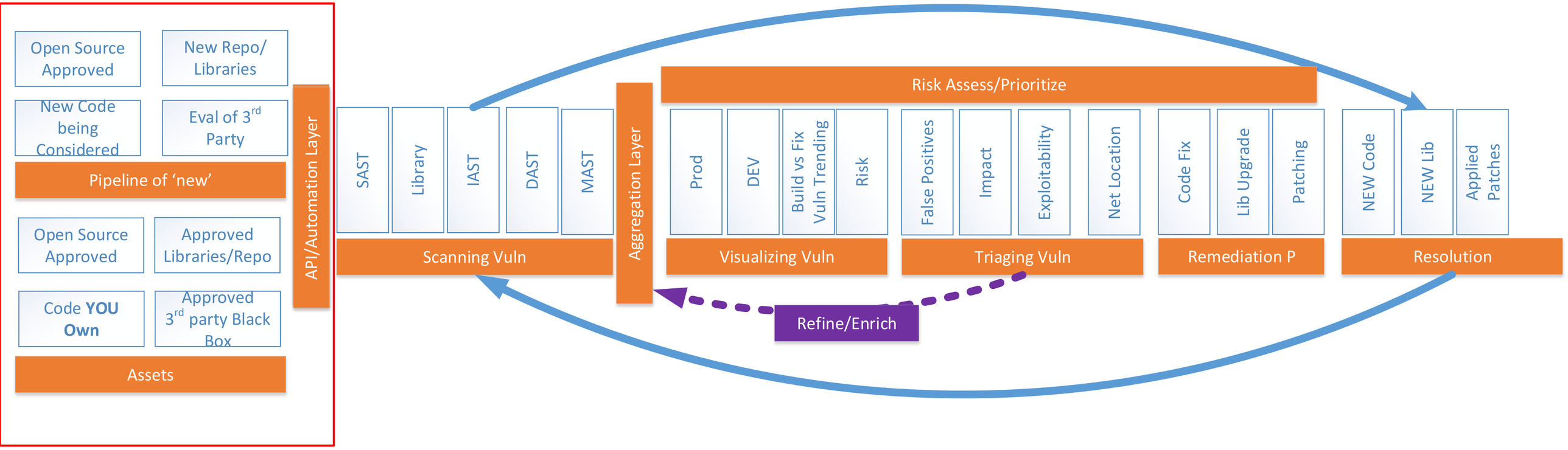
Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

Why do we need to build a strong asset register?

WhiteSource

DEV Security

Production Security



Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

Git to People: Who does what where Visualizer

DEV Security

Production Security

For Every Repo

git ls-tree -r -z --name-only HEAD -- update-tools-mac.sh | xargs -0 -n1 git blame \--line-porcelain HEAD |grep "^author "|sort|uniq -c|sort -nr

List of committers

App scan?

Build vs FIX & Tickets

JIRA

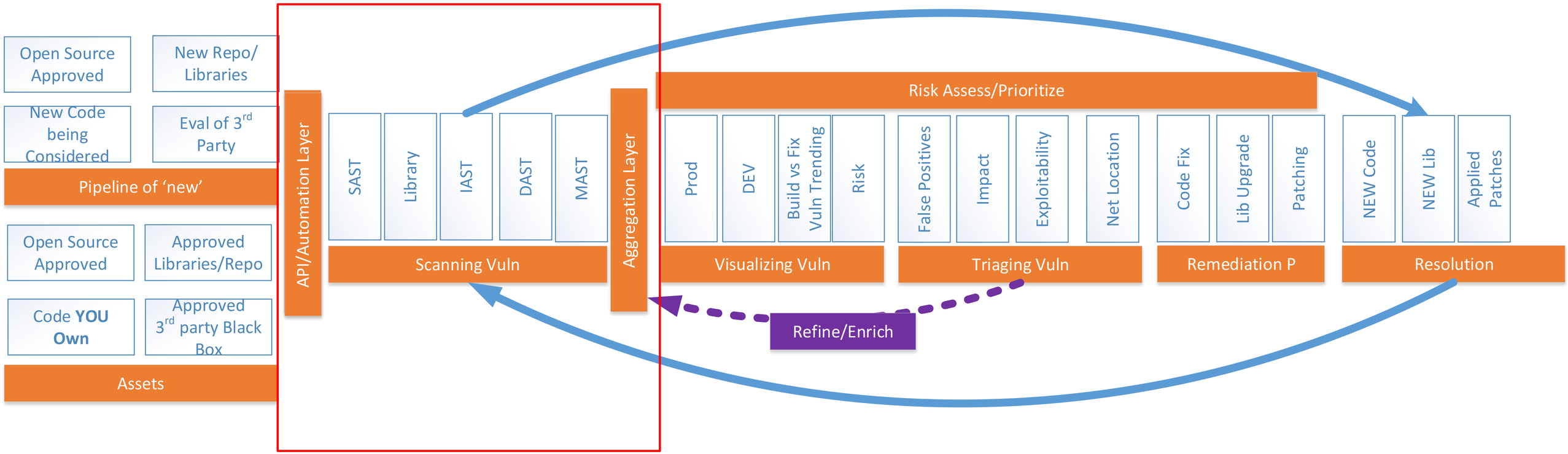
E-Mail/HR DB

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

Dashboard for Code Defects – Part B

DEV Security

Production Security

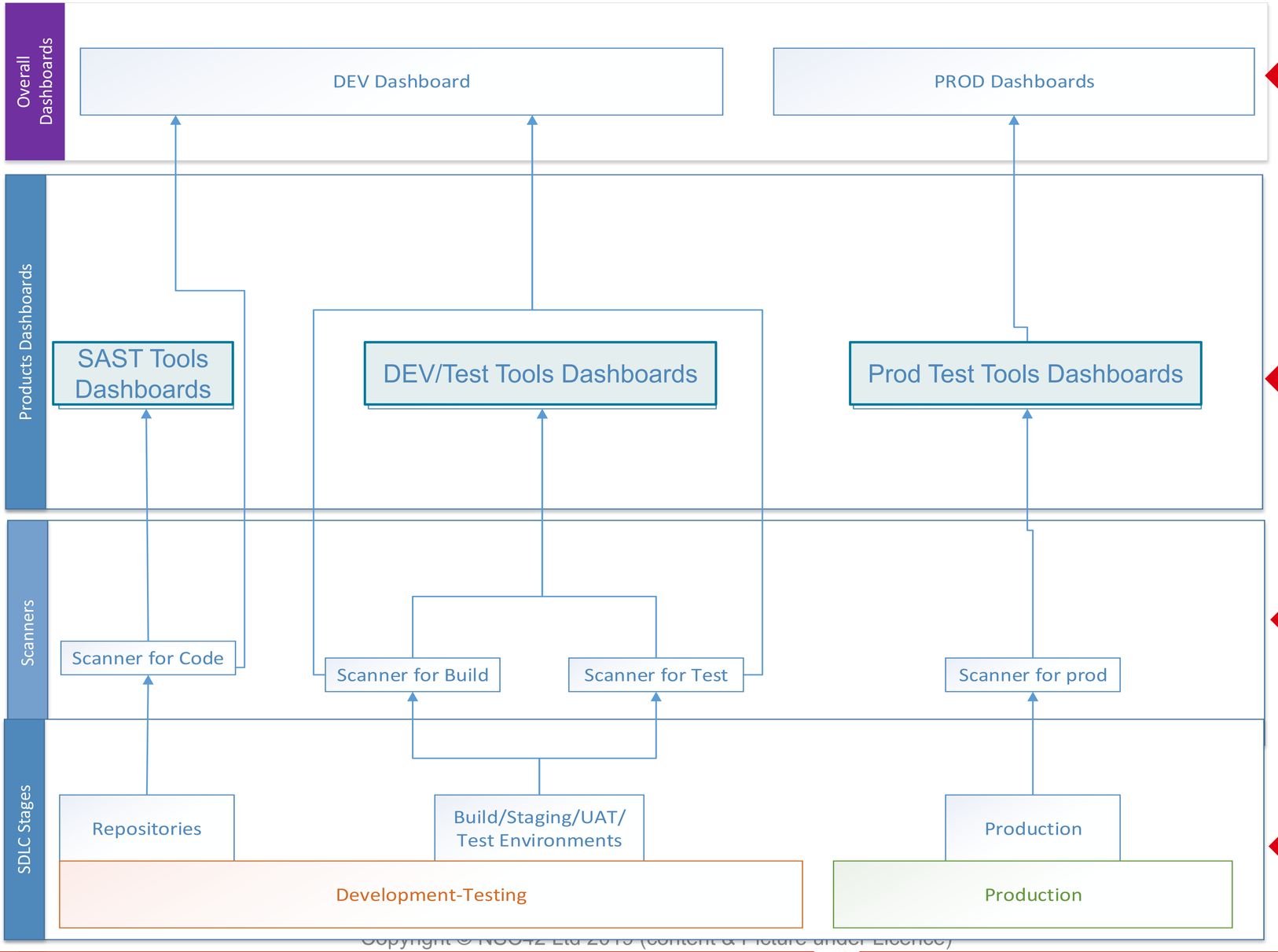


Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

Dashboard for Code Defects -> Under the hood

DEV Security

Production Security



SET Targets For Prod & DEV Vuln

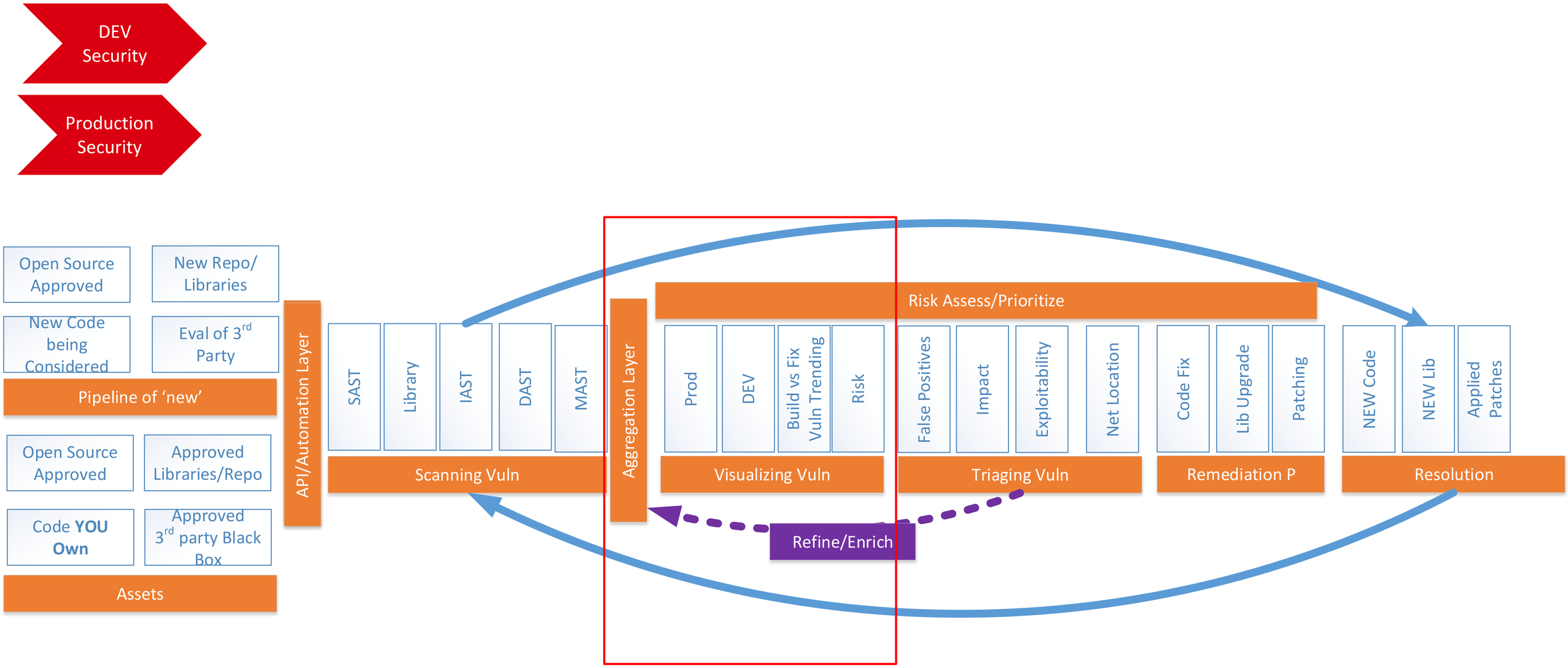
Triage the vulnerabilities

Scanners to Tickets or aggregators

Scan At various Stages

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

Dashboard for Code Defects – Part C

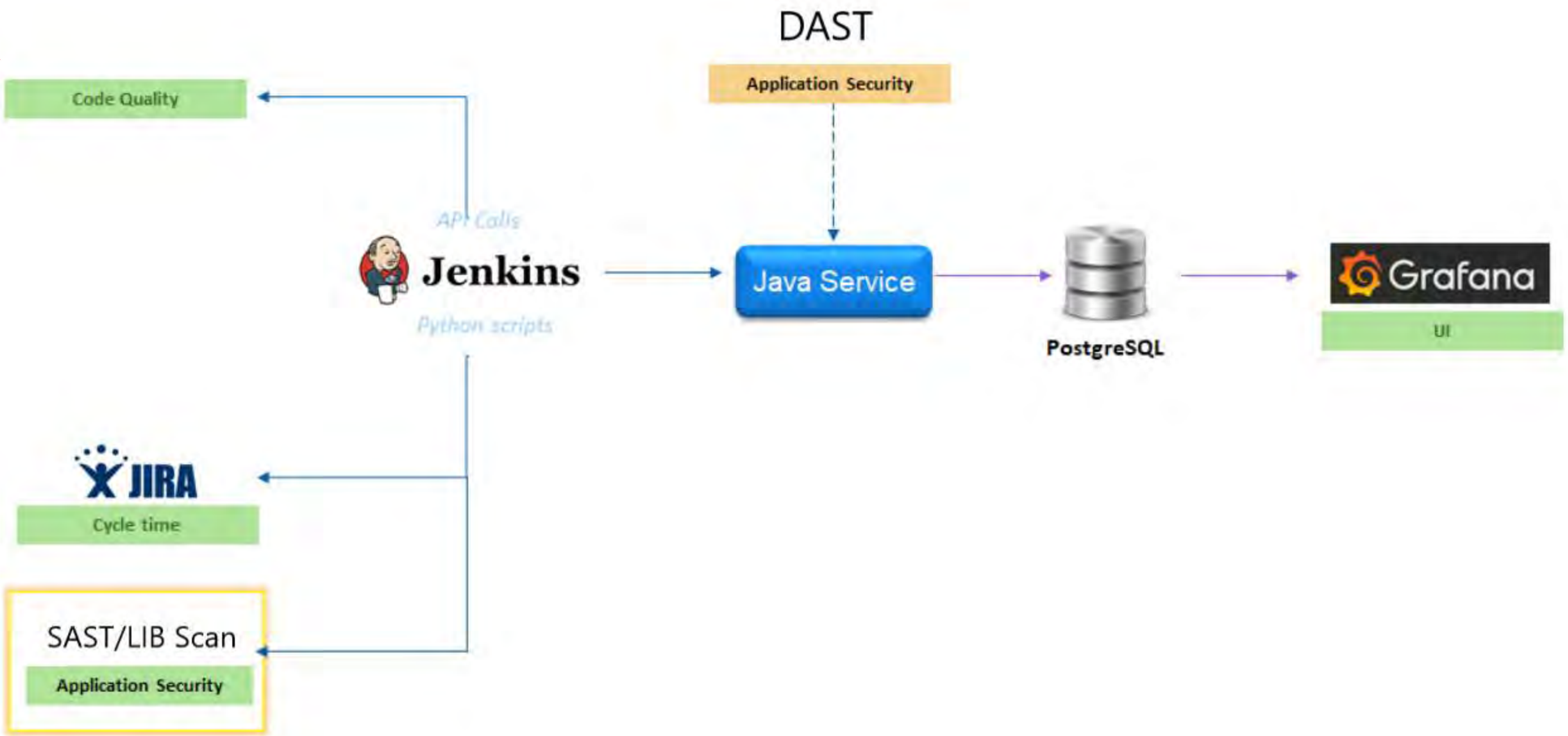


Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

Dashboard for Code Defects

DEV Security

Production Security



Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

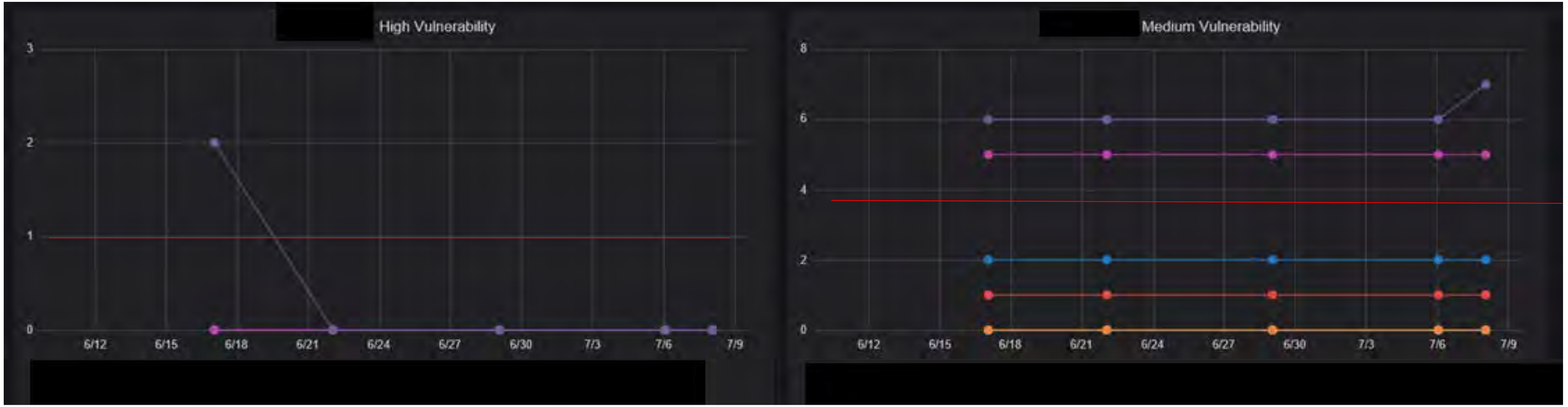
Dashboard for Code Defects

WhiteSource

DEV Security

Production Security

Example of a dashboard for Vulnerability Visualization

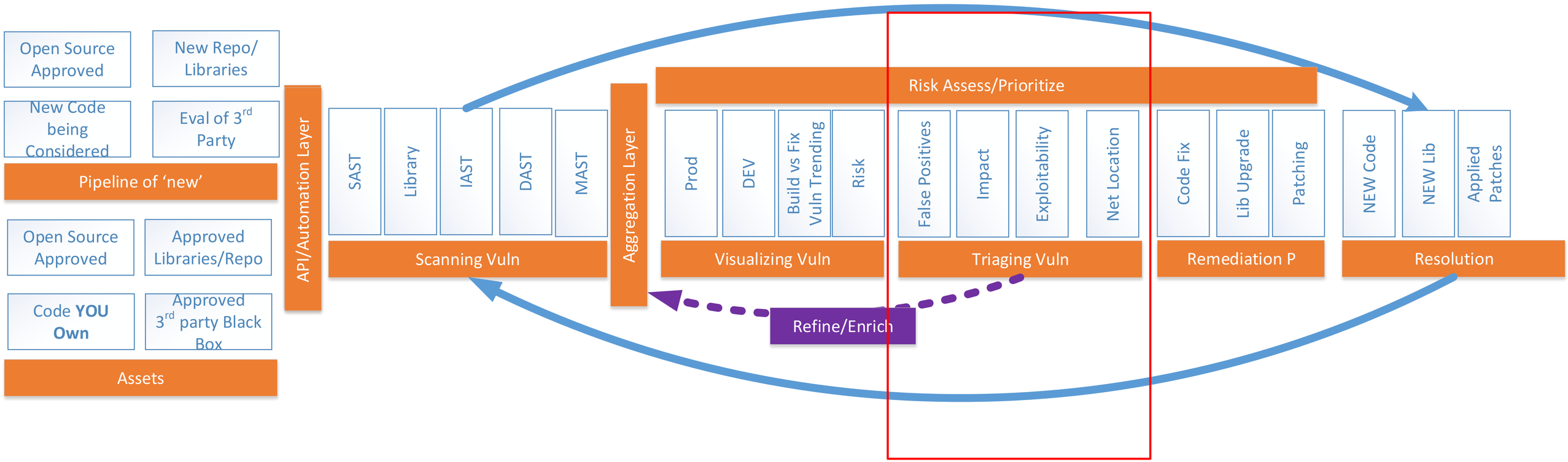


Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

Dashboard for Code Defects - Part D fix

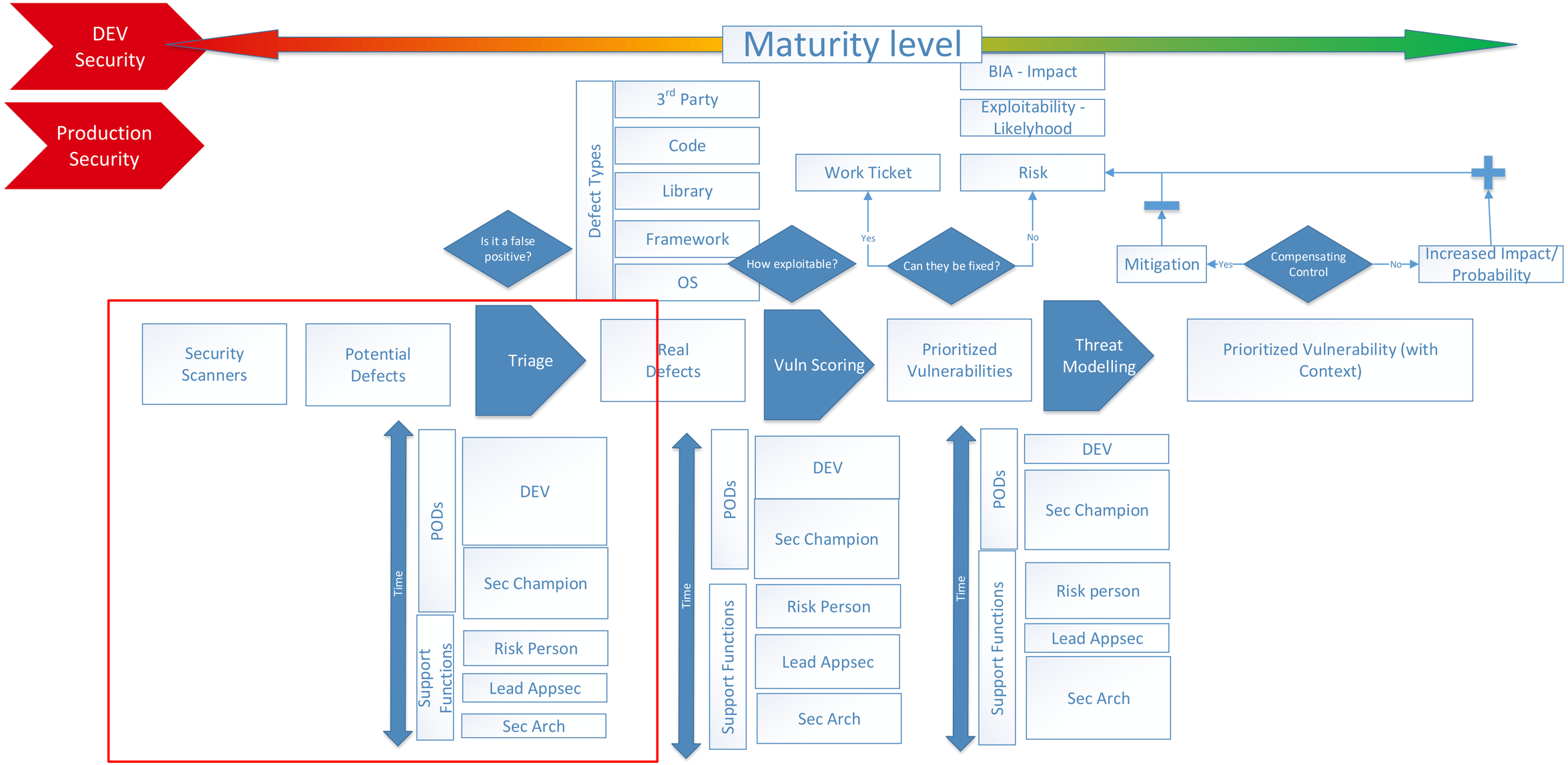
DEV Security

Production Security



Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

Triaging Vulnerabilities



Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

What do you get out of Security Phoenix?

WhiteSource

1. Visualize and Fix Vulnerability at scale and pace (DEV & Ops)

2. Trust the Product team but keep them accountable: Trust & Verify & License to Operate

3. Maturity & Recap

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

WhiteSource

Going fast but with confidence (SEC)

1. Trust & Verify

2. License to operate/code

People & Education

>> Set Thresholds: Bild vs Fix, Vulnerability trending

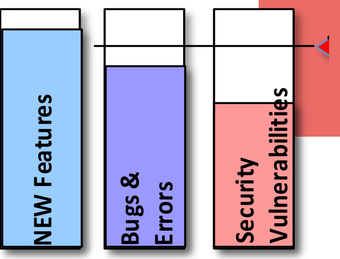
Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

Trust & Verify – Under the hood

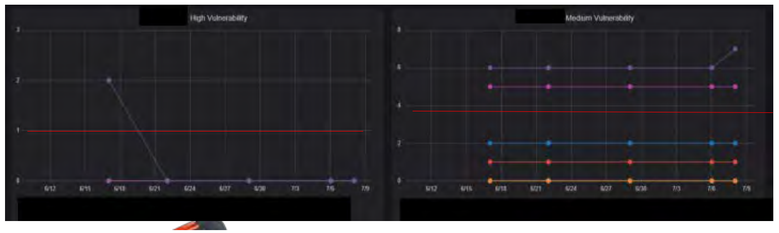
WhiteSource

Learning & Education

Build vs FIX Target



Vulnerability Targets (Quarter)



Phoenix Aggregator DB

License to operate

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

Security Education

Education:

1. Awareness Training For your users

2. Craft Training based on the scanner (faults) data

3. Education on the job – What good looks like

4. Make the training entertaining (CTF and Rewards)

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

Maturity Model & Recap

Bringing all together

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

What do you get out of Security Phoenix?

1. Visualize and Fix Vulnerability at scale and pace (DEV & Ops)

2. Trust the Product team but keep them accountable: Trust & Verify & License to Operate

3. Maturity & Recap

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

To Achieve High Maturity what do you do

DEV Security

Production Security

Overall Maturity

	Level 1	Level 2	Level 3	Level 4	Level 5
	Intial	Managed	Defined	Quantitatively Managed	Optimized
Security Design	AS-IS->TO-BE				
Security Design Governance	AS-IS	TO-BE			
Security Build & Test	AS-IS	TO-BE			
Security Operate		AS-IS-> TO-BE			
Appsec Security Education	AS-IS	TO-BE			
Application Security Risk Management	AS-IS	TO-BE			

Maturity Steps

Maturity	Task	How much
1	No Peer Review	
1	No Code Scanning	
1	No library update	
1	No risk management	
1	No visibility on vulnerabilities	
1	No knowledge of pods	
1	No team to pod mapping	
1	No Documentation of Fixes	
2	Peer Revew	
2	Team to Pod to Stash recorded	
2	Onboarded application on code scanners	
2	Libray scanning	
2	triage of vulnerabilities (base) - Consider only high medium and low	
2	Manual Evaluation of team and Allocation of Licence to Operate	
2	No SLA	
2	No Documentaiton	
2	Adoption Dashboard	
3	Peer Review with Toolset	
3	Updated Teams and asset register	
3	Basic Triage of vulnerabilities	
3	**Code Scan with Pipeline Break & Basic SLA**	
3	Adoption Dashboard (advanced) Per A.C. and Per Region	
3	Risk Assessment from code scanning with record in Risk management Register	
3	Automated Licence to operate: Code Scanning, Libraries, Internal Training	
4	Fix time of vulnerabilities recorded	
4	T-Shirt Sizing of fixes and Adaptation of SLA based on fixes	
4	Visualization of pod to fix	
4	segmentation dev and prod	
4	Fix ticket in Jira & Build vs Fix Concept	
4	Fuzzing (basic with generic per app)	
5	Automated Licence to operate: Code Scanning, Libraries, Internal Training, Build Vs Fix	
5	Automated Fuzzing & Library of tests	

KCI

			Reporting Frequency
	KCI Maturiy	Build/Test	
Prereq ->	0	Who is working on which repository	Monthly
	1	Team On-boarded on scanners (per pod)	Monthly
	1	Code Scanning Frequency per project (min 1 per week)	Monthly
	1	Dashboard for Scanners created	Monthly
	2	Number of vulnerabilities ticket recorded	Weekly
	2	Dashboard for vulnerabilities - Onboarded Projects	Weekly
	2	Vulnerability Fixed (quarter)	Monthly/ Quarterly Checks
	3	Project vulnerabilities integrated in Vulnerability management programme	Monthly
	3	Projects breaching the Build vs Fix target	Monthly/ Quarter Checks
	4	Fixes per thematic in SLA	Monthly
	4	SLA for Fixes (breached/achieved)	Monthly
	4	Team Achieving Licence to operate and Out of the licence	Monthly
	5	Build vs fix	Monthly
	5	Licence to operate	Monthly

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

Fixing Vulnerability the ABC…D

Outcome

Asset Register for	A - IDentify (Software Asset Register)		
	Software you build (repositories)	Software You buy	Trace Completeness across all the application you have
Vulnerability Data Lake	B – Detect (Scan Code)		
	Select Team Leads and identify security champions	Get security Scanners (SAST/DAST) Onboard and teach how to triage	Create a Vulnerability Data lake (results of the vulnerabilities)
KPI Reporting & Dashboard	C – Visualize Vulnerabilities (Display)		
	Reporting Dashboards (based on the maturity & KPI)	Link the trending to Build vs FIX, Vuln trending,	
Prioritizing & Vulnerability Reduction	D – Respond/recover (Fix Vulnerability)		
	7 – Schedule Vuln Fixes (Jira)	7 – Fix Vuln & measure (quarterly)	

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

Conclusion

WhiteSource

Security is everybody's job

DEV and OPS?

- Maturity Model – Measure and define success
- Trust And Verify
- Identify and assess code and production
- Vulnerability Management every day life
- Automation vs people aspect – is a transformation
- Data Driven Education

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

Our Other Services

We believe in an all rounded set of services built on the need of our clients over the years and recognized by the Cloud Security Alliance.

What differentiates our company from other consultancies is that we do what we love and are customer focused.

Our company goes the extra mile in order to deliver solutions that are fit for purpose, effective and cost-effective for your organization's risks appetite.

We offer a range of products within cybersecurity.

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

Contacts

WHEN YOU ARE CYBERSAFE WE ARE CYBERHAPPY

Thank you

Get in touch:

https://www.linkedin.com/company/nsc42-limited

Communications@nsc42.co.uk

www.nsc42.co.uk

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

Copyright © NSC42 Ltd 2019

Cyber Security & Cloud Podcast

By Francesco Cipollone www.nsc42.co.uk/CSCP #CSCP

www.nsc42.co.uk/cscp

@podcast_cyber

@FrankSEC42

www.cybercloudpodcast.com

Sponsored By

NSC42

CSA UK cloud security alliance SM UNITED KINGDOM Chapter

Cyber #MentoringMonday Podcast

Every 2 weeks 1.30 PM UK Time

slack

cloud security alliance UK & IRELAND

NSC42

OFFICIAL (ISC)² CHAPTER LONDON

@FrankSEC42

PUBLIC

Cyber Security Awards

cloud security alliance SM
CSA UNITED KINGDOM

Cyber Security Awards 2020

Cloud Security Influencer of the Year

Submission – 10 of May 2020 (TBD)

Ceremony 4 July 2020

#CYSECAWARDS20

https://cybersecurityawards.com/

https://cloudsecurityalliance.org.uk

Submit: info@cybersecurityawards.com

Info: Francesco.Cipollone@cloudsecurityalliance.org.uk

PUBLIC

Q&A

WhiteSource

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

WHEN YOU ARE CYBERSAFE WE ARE CYBERHAPPY

Thank you

Get in touch:

@FrankSEC42

https://uk.linkedin.com/in/fracipo

Francesco.cipollone (at) nsc42.co.uk

www.nsc42.co.uk

Copyright © NSC42 Ltd 2019 (content & Picture under Licence)