

The Security Phoenix raises from DEV-OPS ashes

A Modern Approach on DevSecOps Focused on People

DevOPS.com webinars - White Source Webinars



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







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** A&Q

2019 (content & Picture under Licence)



About Francesco





Founder – NSC42 LTD

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



We need to make security cool and frictionless

Cappyight NSSC422 td 2200

in <u>https://uk.linkedin.com/in/fracipo</u>



Francesco Cipollone





Security is everybody's job





What do I usually talk about?

Appsec



99 little bugs in the code. 99 little bugs in the code Take one down, pate

127 little bugs in the

Copyright NSC42Ltd 2020



What the hek is **DEV-SEC-OPS**?

What kind of animal is the DEV-SEC-OPS? Integrate security into the OPS team (and add a spark of RISK)



Copyright NSC42Ltd 2020

in <u>https://uk.linkedin.com/in/fracipo</u>

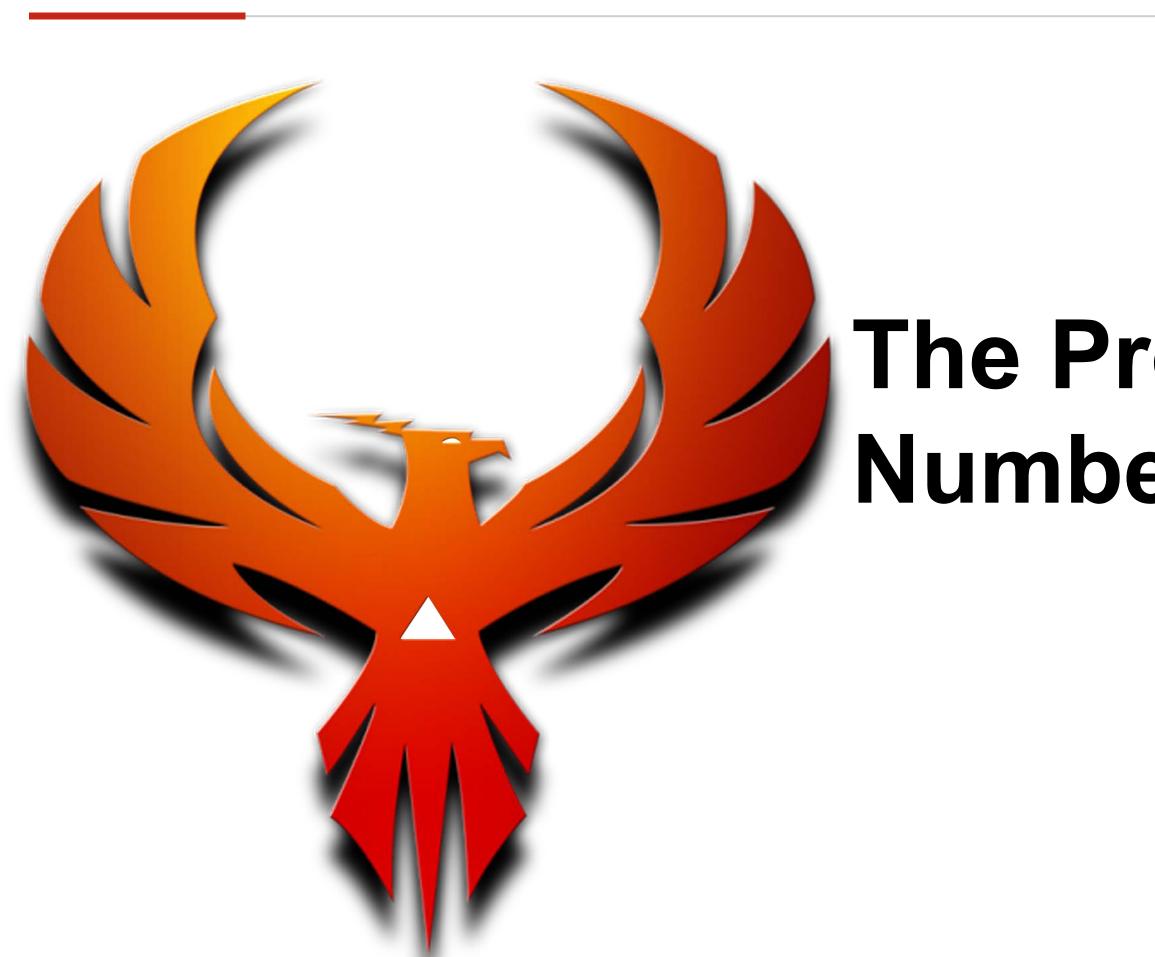


Copyright © NSC42 Ltd 2019 (content & Picture under Licence)









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

Copyright NSC42Ltd 2020

in <u>https://uk.linkedin.com/in/fracipo</u>



The Problem Landscape: Numbers behind the breaches

Why do we worry about security?





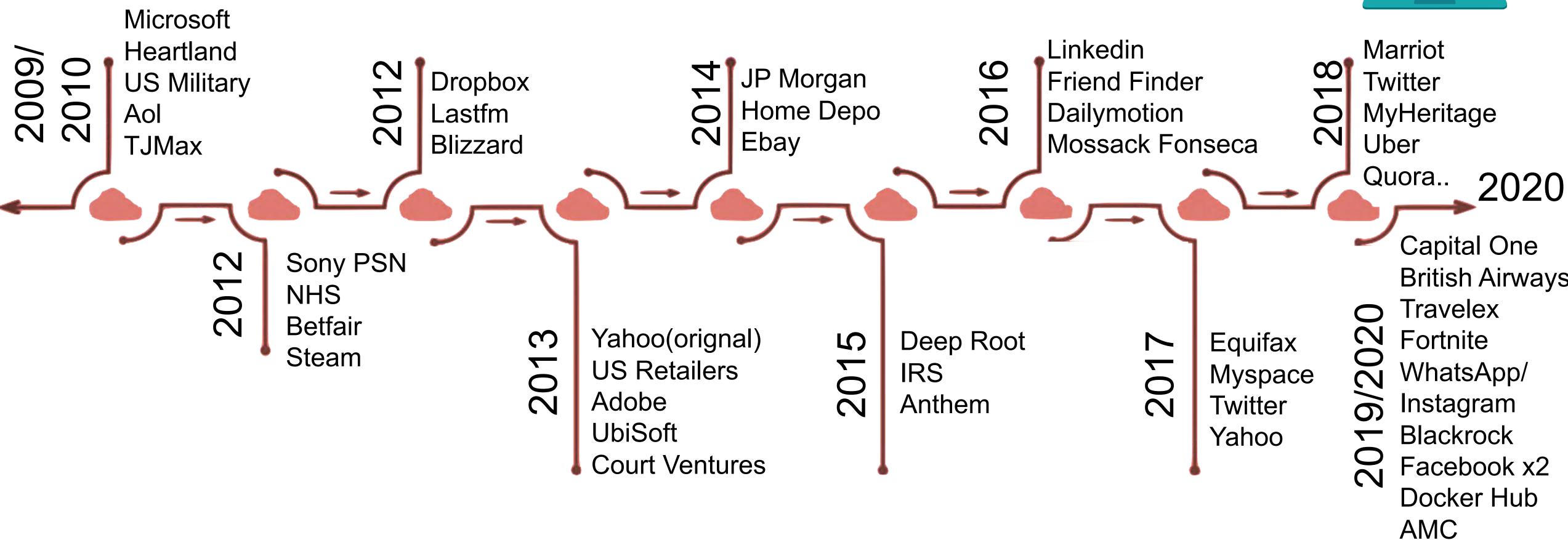






Major Breaches over the years

Why fixing Security Vulnerabilities is everybody's job? ... because we all get affected by it



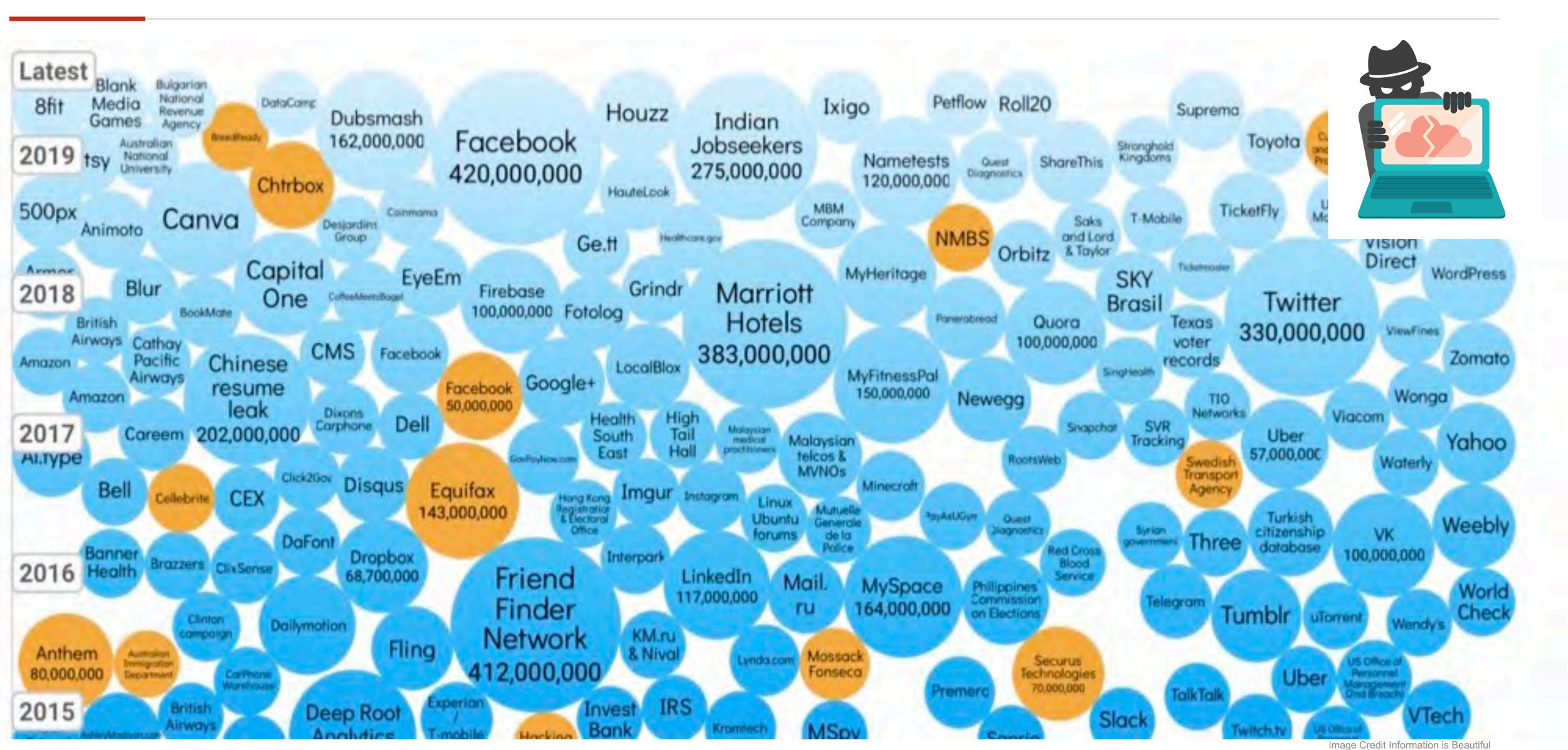
Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

Copyright NSC42Ltd 2020





Major Breaches



Copyright NSC42Ltd 2020

in <u>https://uk.linkedin.com/in/fracipo</u>



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

www.nsc42.co.uk

TOP 5 Security Breaches

Capital One (2019)

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

Marriott (2018/2020)

Second time access breach after 2018 hack

Nintendo (April 2020)

Credential stuffing from previous hack

British Airways (Sept 2018)

Injection of code in a library

Microsoft & Facebook (2018-19)

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

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

2

Copyright NSC42Ltd 2020

in <u>https://uk.linkedin.com/in/fracipo</u>



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

@FrankSEC42

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.



Malicious Actors

Well Known/Hacktivism

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

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

Copyright NSC42Ltd 2020

in <u>https://uk.linkedin.com/in/fracipo</u>



Financially motivated

Gold Southfield-ReEvil, Magecart, Lazarus group ...

Less visible more dangerous









Breaches in Number - appsec

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

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

Every 36 minutes

A new security vulnerability is identified

It takes **150-180** days **3-15** days

To fix a vulnerability

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



Av Cost of data Breach 3.03 m

N. Of Vuln per year **1400** vuln

As disclosed vulnerabilities

It takes

@FrankSEC42

To exploit a vulnerability

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? Every min 62K record disclosed Record per minute disclosed Data breaches 80% due to misconfiguration Cloud misconfiguration is

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

dominat



Total cost of breaches 5 trillion \$ / 4 trillion GBP

N. Of Vuln records 33 billion

Disclosed records over 1 year

Av. Cost per record 150\$ per record

Average cost per loss record

@FrankSEC42

www.nsc42.co.uk



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

1X

Requirement Architecture

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



Cost to Fix vulnerabilities 30X 15X 10X 5X System Acceptance Production/Release Coding Testing





Copyright NSC42Ltd 2020

Copyright © NSC42 Ltd 2019 (content & Picture under Licence) in <u>https://uk.linkedin.com/in/fracipo</u>

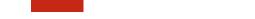


The Security Phoenix Appsec Program based on Data and People



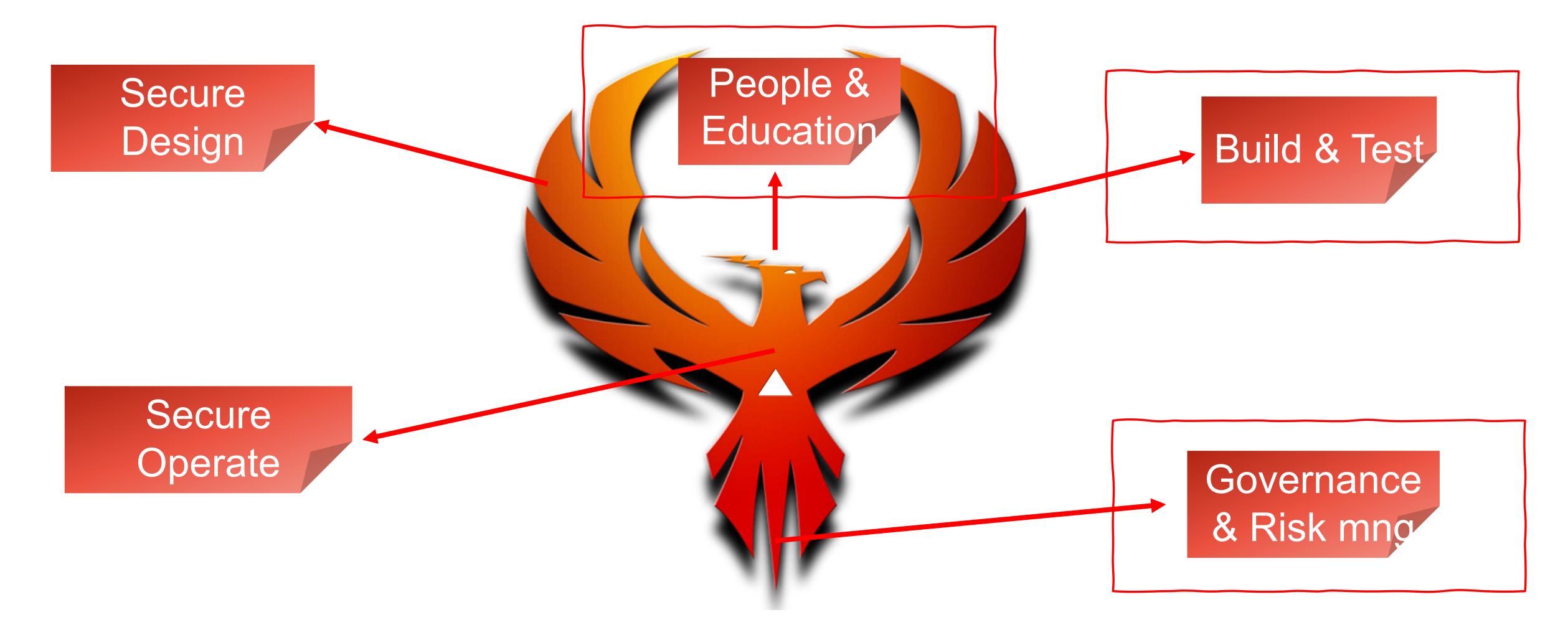






Anatomy of a phoenix

What Are the core pillars of Security Phoenix



www.nsc42.co.uk

Copyright NSC42Ltd 2020

in <u>https://uk.linkedin.com/in/fracipo</u>



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







Evolution?

How do we get better and measure it?



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

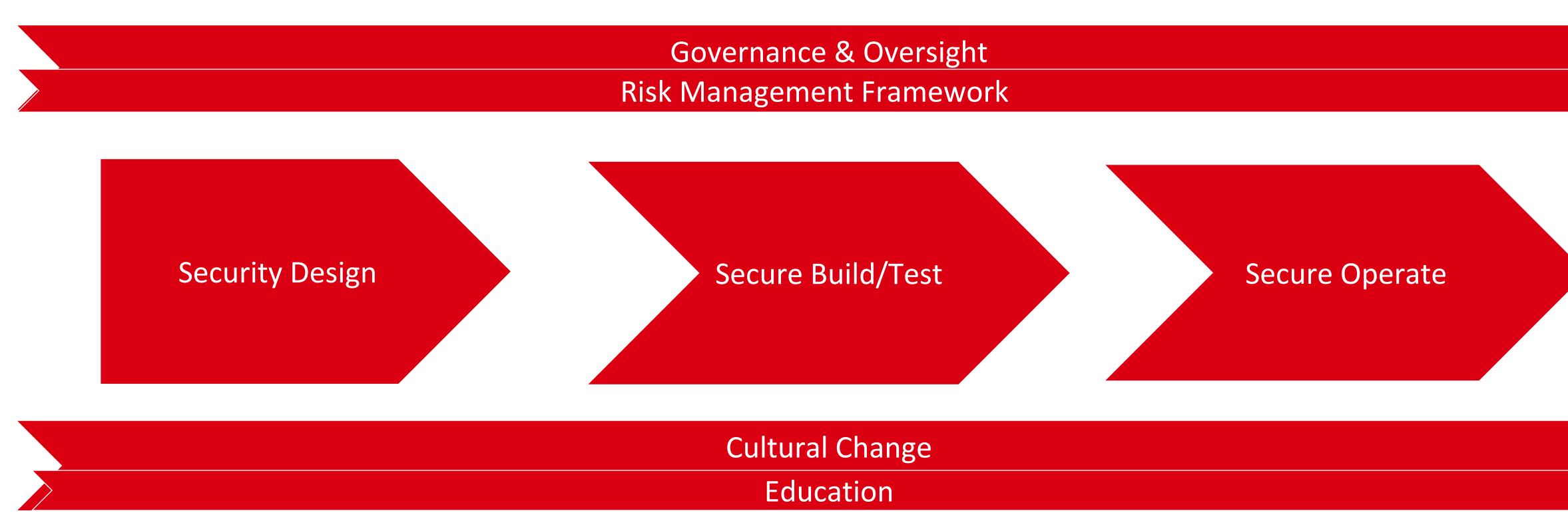
Copyright NSC42Ltd 2020

in <u>https://uk.linkedin.com/in/fracipo</u>

www.nsc42.co.uk







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

Copyright NSC42Ltd 2020











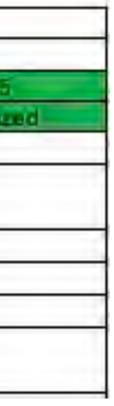
		AS-I	S		
Time	2019				<u></u>
	Level T	Level 2	Level 3	Level 4	Level 5
	Intrai	Managed	Datined	Quantitatively Mar	Optimized
Security Design	AS-IS				
Security Design					
Governance	AS-IS	-			-
Security Build & Test	AS-IS		1		
Security Operate		AS-IS	19-1		
Security Education		AS-IS			
Application Security Risk Management		AS-IS			

Copyright © NSC42 Ltd 2019 (content & Picture under Licence) in <u>https://uk.linkedin.com/in/fracipo</u> www.nsc42.co.uk @FrankSEC42

Copyright NSC42Ltd 2020



	TO-BE								
Time	2020			1	-				
	Level 1	Level 2	Level 3	Level 4	Level 5				
	Intal	Managed	Defined	Quantitatively Mar	Optimus				
Security Design	10 m	TO-BE		10.00					
Security Design Governance		TO-BE							
Security Build & Test		TO-BE							
Security Operate		TO-BE							
Security Education		TO-BE							
Application Security Risk Management		TO-BE							





	Gibwemanke	2	ikk Managmern		alaret Des	alan.			Secure Build/Test
-	Colouri Ind	August Carp # 14	and had had	-	North	-		-	45 344
		SRA M.E.			11		Natio.		
SELA DE LA	A & Card Disease small below it is mile			-		Tortan summer perif	NLUK.		Enforteries
IN CO IN CO							SILM		State and an
-		25 A			1	No and Long	NUMBER OF		No loss of the
19/24 G	The second secon						Sittle	-	
mu la	Calcillation of some second to be			-			NULLY-		No longitude of suit
10224	East New York Complete Development					1	Siladi.		Contraction and manual
1413 M	tions (Build out match school and the					1	WAAM.	- 1	Saling and a Char
-	Test of same trian intelling								
					- 12-2	And and a state of the		-	
	Estampi Antincine			-	-	And and Addressed	NIAAA	-	Distort
1 4	Includence				2.1	Youth	53.59		Total to Fait in Sandy sociality (NYS %) Descention
2	These Client Architecture		-		12	Test Constant	Saide.		Entirementari applicamentari produ
4	Dans Array Million				1	Design and	TO NAME	-	line
	Date & December 1978 Access				1	Con a Descent SHE	Keluul.	-	shape of Subsections, Bairs;) Consider only bits section and fee
	control encount		1 (· · · · · · · · · · · · · · · · · ·		12	in the second second	SALLS.	1	Minuted Addressing of Linkson for Unsure
0 1	Dani stat Ataan		3	-	-	Constantial in success	NAME.	-	Sec. B.A.
a 5	Doosen Revealed			1	1	Terme Arrester	NIAM,	-	No Despension of task form
	Track Sales Modelling	A CONTRACT OF A				-	NIAA		Adapter Disbload
	Delawar of Chart				2	Provide State	NAME OF T		Roo Carries Stat Circuit Yout
2	Romit Arkinson A	and some first states			12	Anna Antonia a	Salata.		Montal allocates of even \$10.4 in: in call address
10 1	Terro Monteller				2	They Budden	TAKA -	-	Deput Vendence De Mand
							121		Name and Address of the Owner, Spinsor
	P.D. Sec. Treatment					1/	NALLE TZI	-	Bookener and Solar
		and the set of the	3				NEAL .		Contactili Park Stands Records
	Products have to combail 10 for summer			1	1	Number 2 Copy in constant, Street,	NILAM, T24	-	Rate Res distantions
	Parase Manage - Paraset Paraset			-	N.	formation from the	tai		Cole Russ with Pepulae Establish Ratio RA
	from Many . Its second faires	A			10	And they avoid from	12	-	Adoptin Distilicial Infrances Per A.C. and Performer
2	Form Harm - Arlinson Parton				1	Party Street Articles Party	127		Rink Astronomi than only incoming with Report in Defensi
	Bad sections for Section 5.				4	Red parents from Reason	NAME .	-	Assessed Diverge is sense 17 sde
- 14	for first on Parallel of call second from the				1	Marco Providence	2014A		To be distanting south
21	Californi (Carmala				11	Characteristic	WILLA.	- 1	Titles living at thest and Adaptation of Advanced on Press
2	Trainman disarra		4		-	200000	10	4	Vanitoine direite it
100		and the second second					120		Annual State and State
					1		PRALLE.		Printer arready mail on Pro-
	1							-	Canad
	 12.4 		2		-		THE THE	-	Faces first with some start
	2.12.2.2.2								
			4		-			-	
	and the second se			1.000		Name and Advanced of F	-		Assessing Lanser, or opening Code
21 24	Monomore a continue to party			-		tores.			Read Processing States and Volt
				-	-	-	Taila.	-	Advertised Discourse
							20	_	the set from
				-	-			-	

Copyright NSC42Ltd 2020

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

 in
 https://uk.linkedin.com/in/fracipo
 www.nsc42.co.uk



-			Secure Operate		r				Secure Elucation		
1	See	-		Į,	-	B-COMPA		1464	Notes L	11	
,	1.120				NAME OF			1000	1 C		
2	and o		State bar	1	NIKKE						
Ē	uut o		No Park		HOLDINAL P				No American man		
Ē	avar.o		to Result		HEART			-	No. of the local dataset		
Ē	an a				NAME			1			
B	TAXE OF		warmen and								
Ľ	autéro.		No with installar second						1 Common (1997)		
1	ALC: N		For Descinante Intel	10							
1	RAMES.		Non- Million			1					
5	BAAGO		Safes			1.771		-			
	44410		Grant Real Printers & Street,		SOLUM: B			-	term for barren		Characteristics of the Maturity
1	akatus 2		design and have been		NEADER			I.;	1149 Juint		onaraoteristics of the maturity
1	ajutaris 1		Problem Deviding		NEUMOR.		2	1.00	Same Carlo Want & W.		
1	SUAL PROPERTY		to here division them.		NAME OF				Mental and Designation		Level 5
1	stuin.	-	No Later In case		SHOKE.				Keep Tartis		Optimizing
1	auarn		Denne		No.44.P				de Wald Internet	1.1.1	
	SM IS	2	Concept State		NIMAR			1	Same and	11	
1	ante o		harmonic bines dourses	12				1-14	a second s		Level 4 Pro
L	1.1			1		25.1		Dec 14	1 mar 1 mar 1		Quantitatively Managed an
I				19.2				1	12		
		-		1		1 100.4					Processes character
	-	1.1				1.001		1.1.1		11	Level 3 organization and is
				1			1				Defined (Projects tailor their proces
1	ALLE O		Da Drawni Isan Kirawa	112	NEALAR.P.		10		Red midstern		organization's standards)
2	ali Marini T	-	Variable According to the	1	TODUKA:			1	Second Character	1.1	
	0.446		Winner wanted	1.5	NUKALE			1000		1.1.2	Level 2. Processes characterized for p
- 14	aluto -	- 3	Programme and a second state	1	NAMES		-	L	Chantel		Managed and is often reactive.
1	avaria		Manual Income of Street, or other	100	NEARE		1.	1.1	Undborgan	1	managea
		1	a la constante de la constante				.,	2.14			
1								1	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		Level 1 Processes unpredictable,
12	ante o	-	Parties Long and R.A.		SILOR.P.		1	2.11	Annual Grant Street		Initial poorly controlled and reactive
1	avar n		Al-Patrice		SHALE-			-	Rich & Country Do sume		millia
t		-	Starth Autorithmation	-	28	-			Instruct First Frank		
ľ	ANE O	- 2	DEV/red		Solicia la 2			10.00	OVAP here:		
2	ANEO		Riss		SECRE.			1.17	Minute approximation property and		
ł	ane o		And Bernell					0.1			
k	NUKO		Volacobilities visualities and appropriet with application years.								
Т	auco		1000								
ŀ		-	Fight in Proceedings		-			-		-	
	ALC: NO.		and the second		REURA						
12	SALK O		Les Artist provide lines		20 MAAAFE			-		\square	
4	6 - · · ·		Pater New Yorkstown		26-				-		
10	NALE O		Manual Bant III for balancehilinity		NEAR II 20 SILANCE	<u> </u>		-			
Ŧ	2		Sad allos annal		28	<u> </u>					
2	antes .		Auto Income in operate Lowening. Radial on Pro. Value Stand are surgered		SOLATE D						
1	instants -		No Depleyance systems this surface approximation		NEQUE:					211	

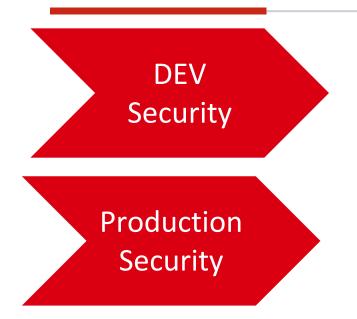


levels Focus on process improvement cesses measured controlled rized for the proactive.

ses from

rojects





Overall Maturity

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

Maturity Steps

	Mat		How
	urity	Task	much
		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	
Maturity	2	triage of vulnerabilities (base) - Consider only high medium and low	
-	2	Manual Evaluation of team and Allocation of Licence to Operate	
el 3 Level 4 Level 5		No SLA	
Quantitatively		No Documentaiton	
ned Managed Optimized	2	Adoption Dashboard	
ica Managea Optimizea	3	Peer Review with Toolset	
	3	Updated Teams and asset register	
		Basic Triage of vulnerabilities	
		Code Scan with Pipeline Break & Basic SLA	
	3	Adoption Dashboard (advanced) Per A.C. and Per Region	
		Risk Assessment from code scanning with record in Risk management Register	
		Automated Licence to operate: Code Scanning, Libraries, Internal Training	
		Fix time of vulnerabilities recorded	
		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 Copyright © NSC42 Ltd 2019 (content & Picture	e unde
in <u>https://uk.linkedir</u>	<u>1.CC</u>	m/in/fracipo www.nsc42.co.uk	9



KCI

			Reporting Frequency
	KCI Mat rutiy	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

Fr Licence)



The Visibility Problem From Dev to prod and cakes

Copyright NSC42Ltd 2020

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











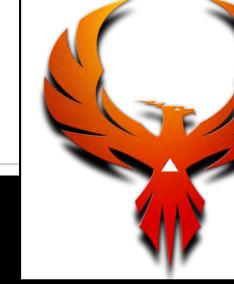


Understanding the room you walk in – Asset Register



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































The Problem Traceability Problem The software security cake

Copyright NSC42Ltd 2020

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















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

The Objective of the various areas are **Combine ingredients (libraries+Code)**

- Bake the cake
- Test the cake •

Act as Health Inspector

- (from asset register)
- Test the cake for mould





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





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



Build/Test

Security Build & Test

That the cake is made up of genuine ingredients

20



The Appsec Lifecycle & Shift Left The Software Asset Register

Copyright NSC42Ltd 2020

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

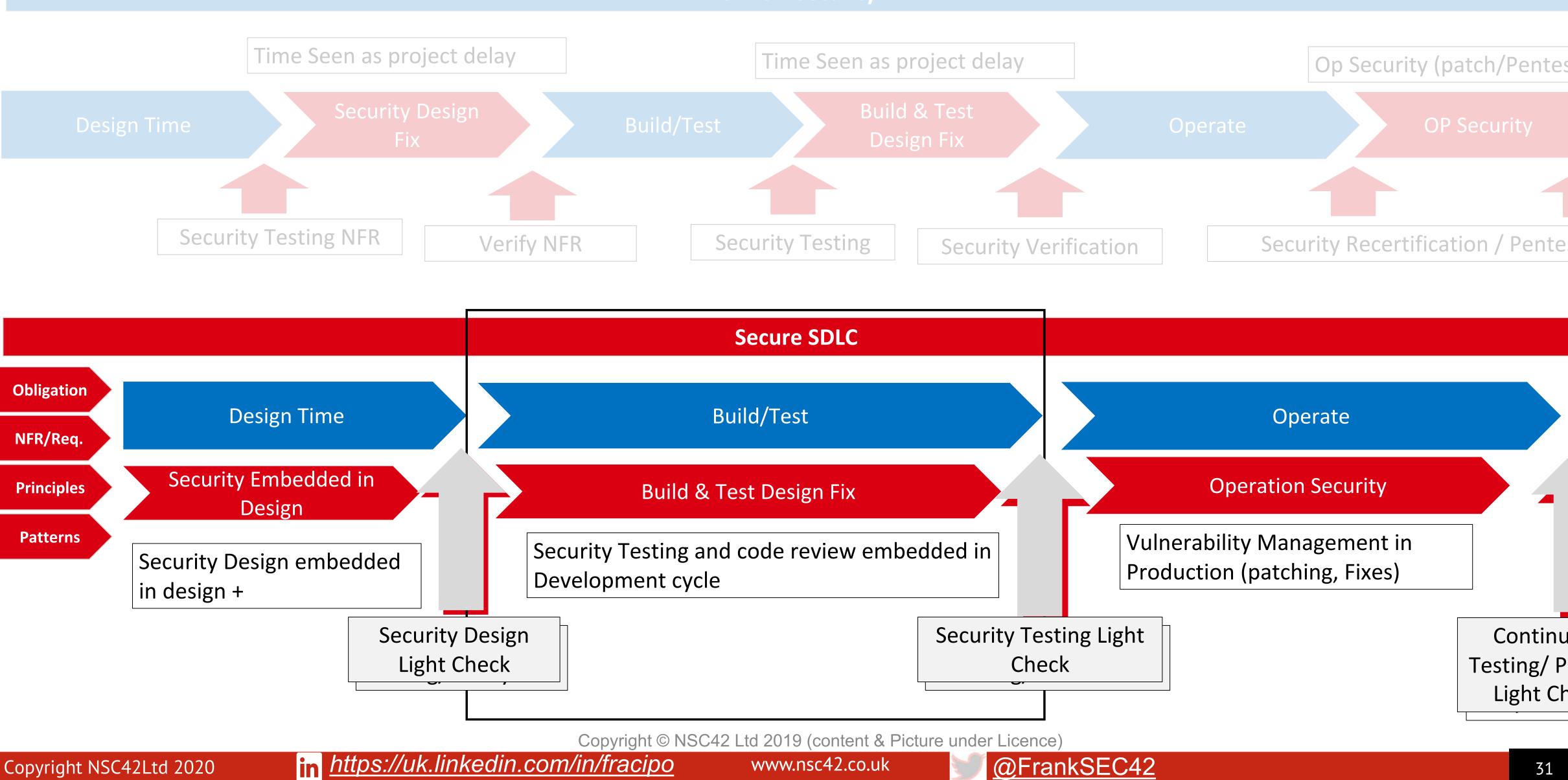








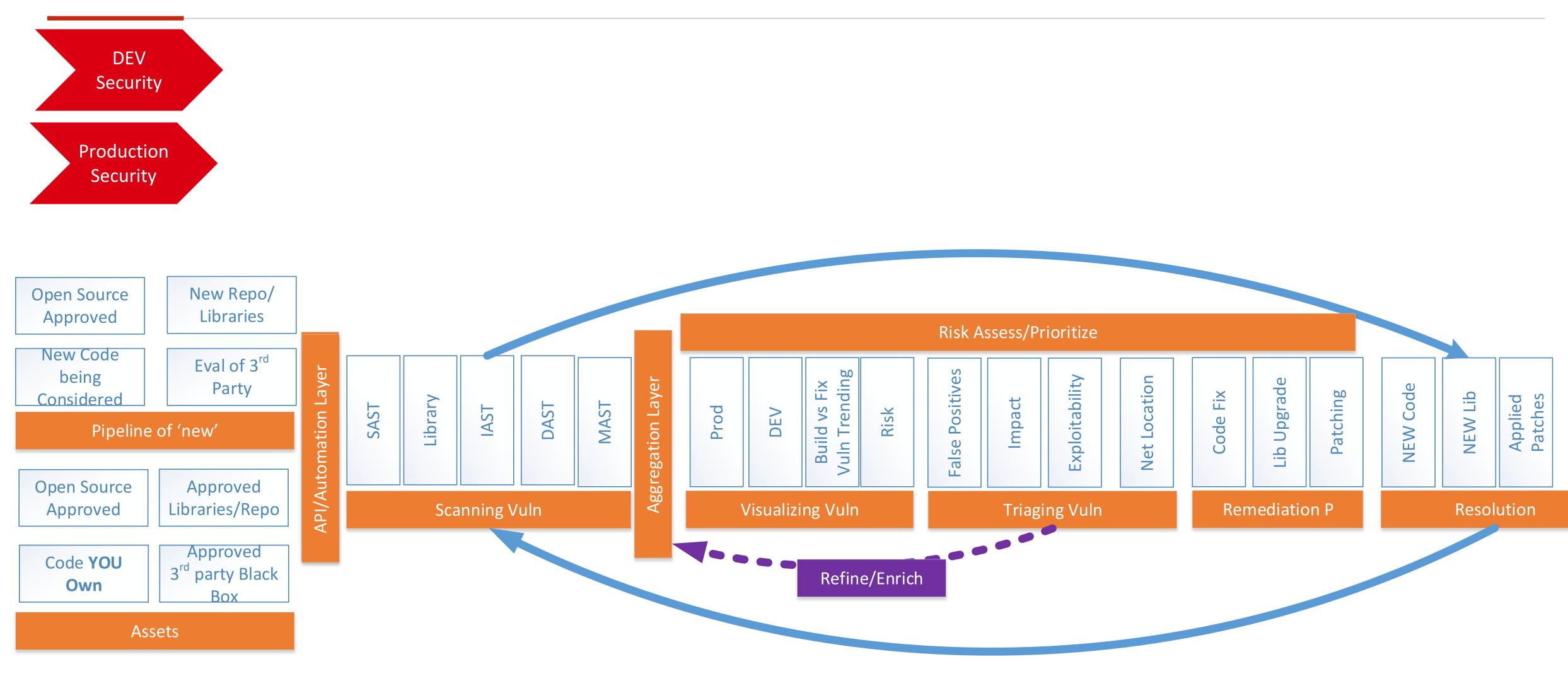
Shift Left - Meaning





test)	
test	
nuous / Pentest	
Check	

Lifecycle Explored



Copyright NSC42Ltd 2020

in <u>https://uk.linkedin.com/in/fracipo</u>



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





Solving Visibility and Traceability Problem

Copyright NSC42Ltd 2020

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

in <u>https://uk.linkedin.com/in/fracipo</u>



Vulnerability management











Vulnerability management Definition

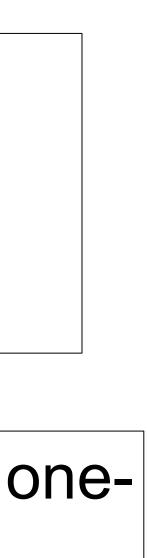
"Vulnerabilities can be discovered with a vulnerability scanner, which analyses a code or system system in search of known vulnerabilities, such as code defect, insecure open source libraries, insecure software configurations, unpatched systems"

Vulnerability 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.



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

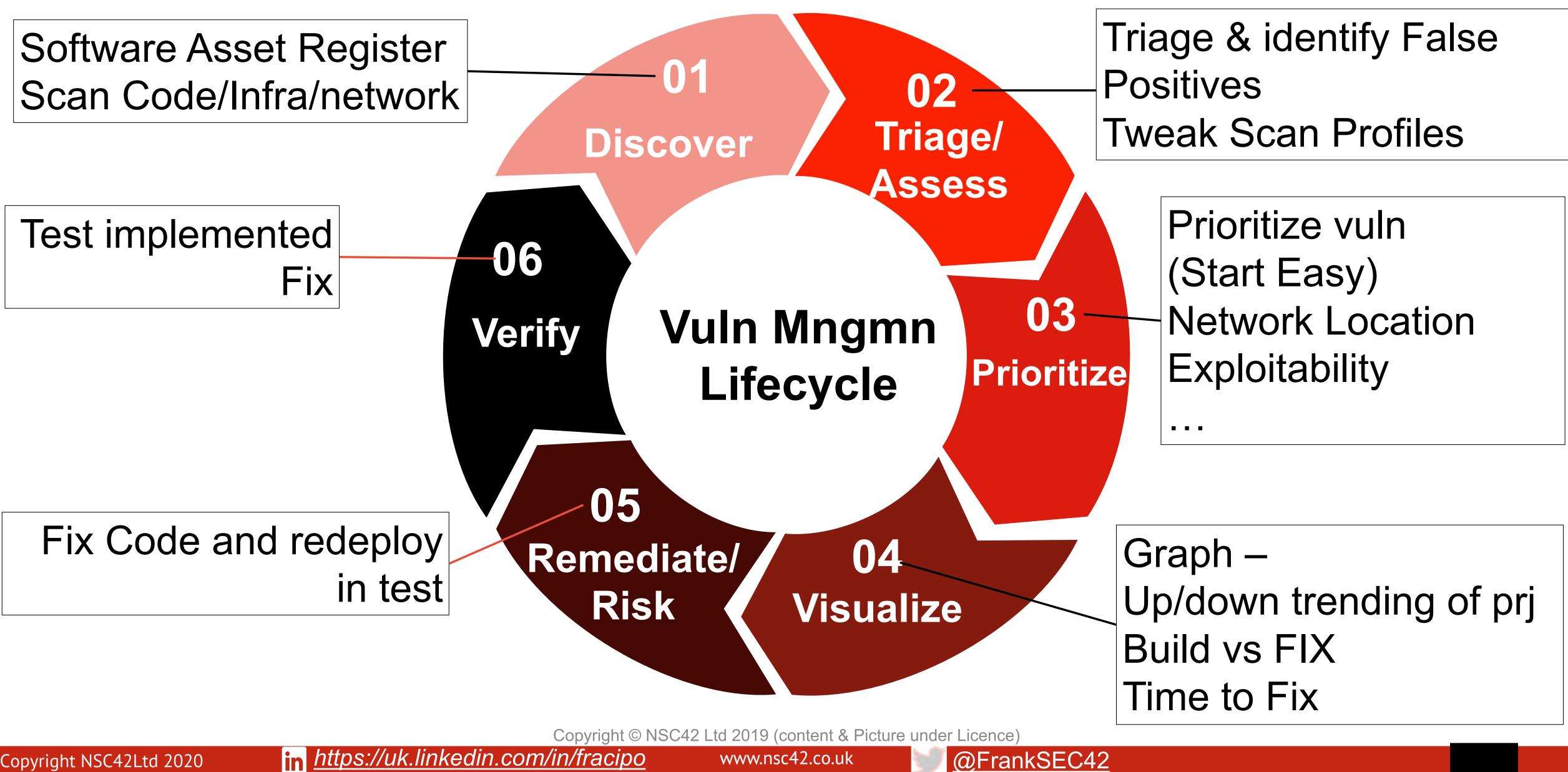








Vulnerability management Lifecycle



Copyright NSC42Ltd 2020



Fixing Vulnerability the ABC...D



Software you build (repositories)

Vulnerability Data Lake

Select Team Leads and identify security champions

KPI Reporting & Dashboard

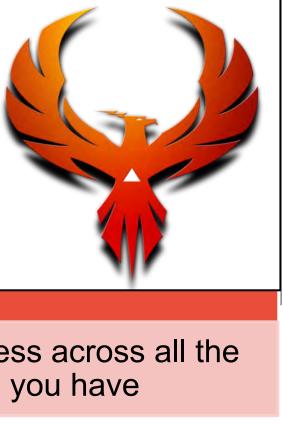
Reporting Dashboards (based on the maturity & KPI)

Prioritizing & Vulnerability Reduction

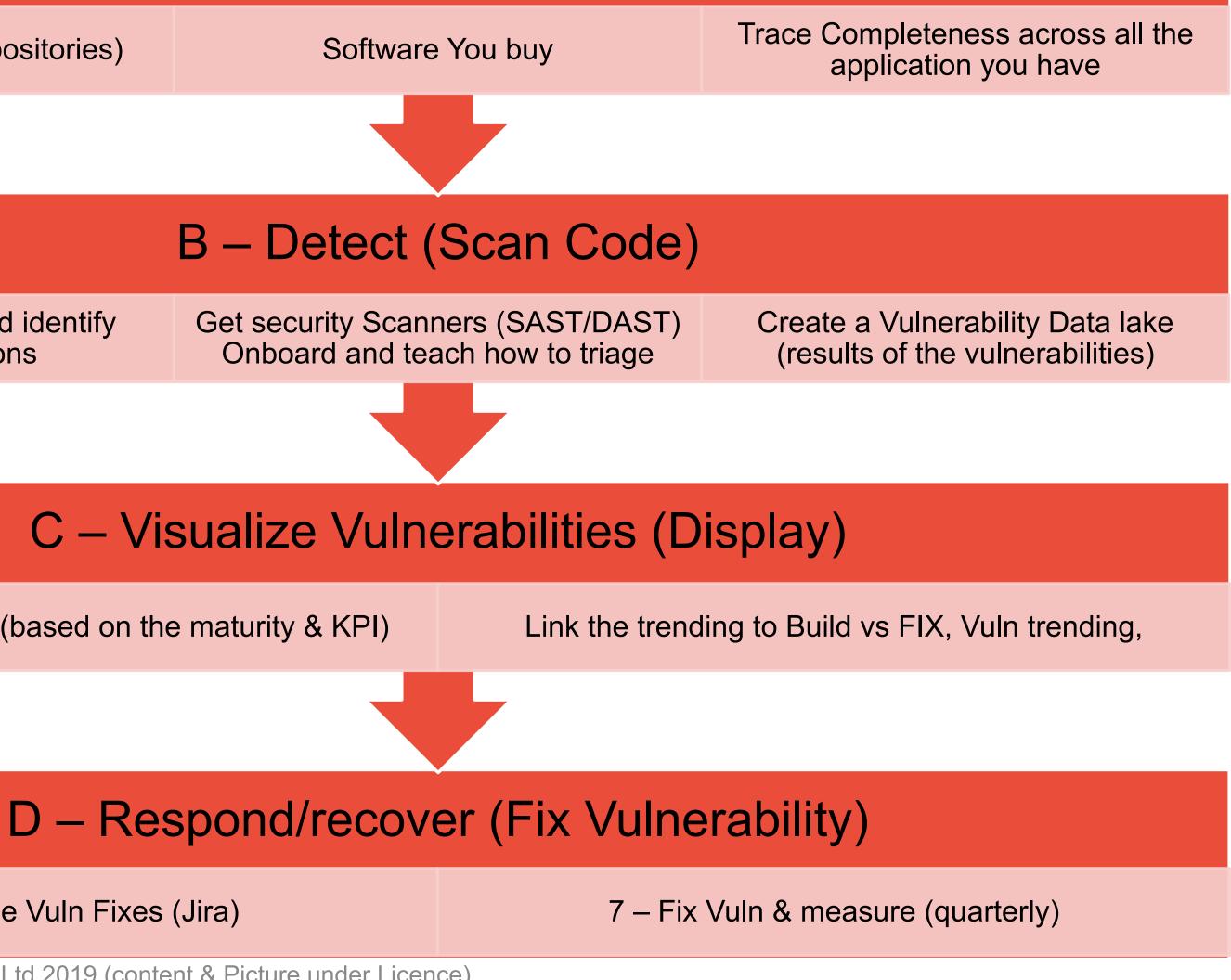
7 – Schedule Vuln Fixes (Jira)

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





A - IDentify (Software Asset Register)





The Traceability & People Visualization & Accountability without finger pointing

Copyright NSC42Ltd 2020

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







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)

Copyright NSC42Ltd 2020



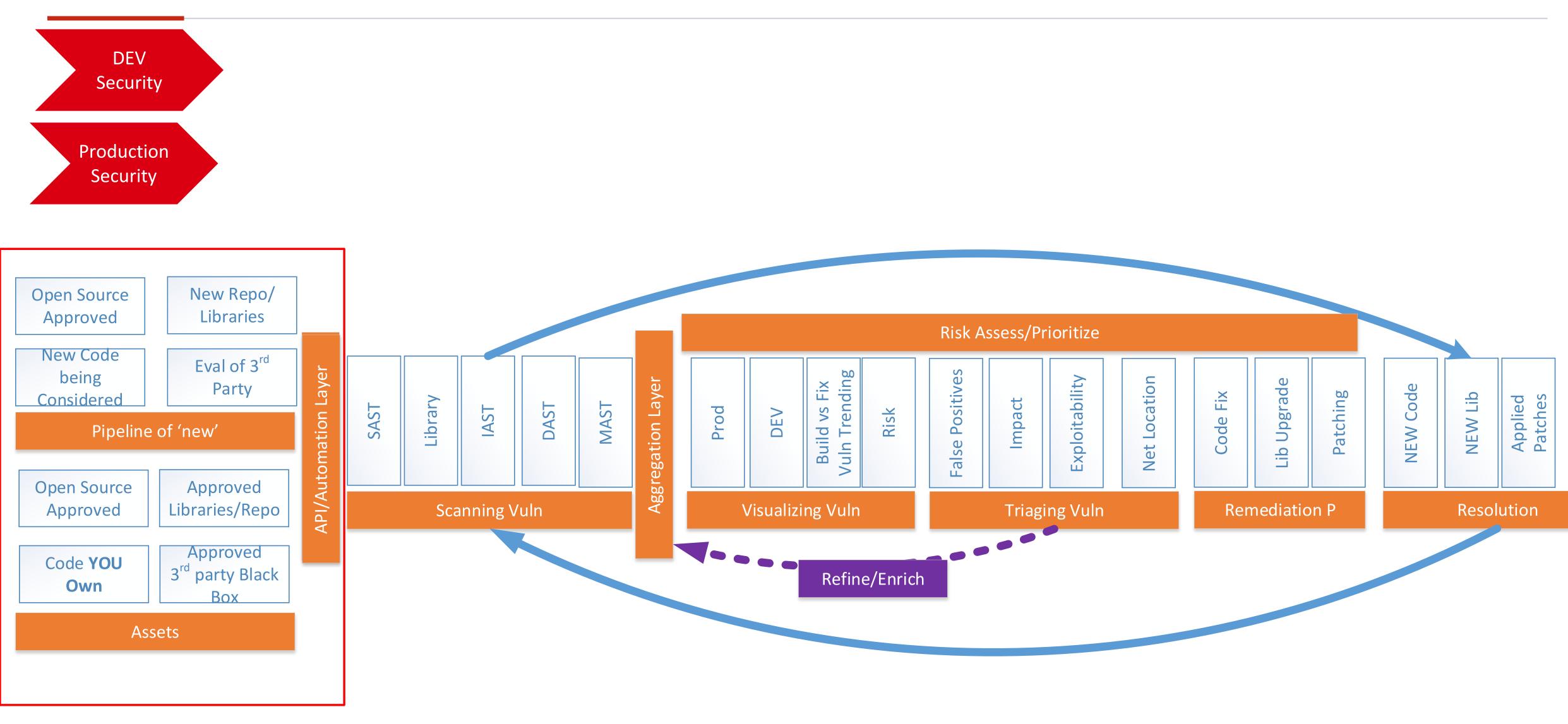








Why do we need to build a strong asset register?



Copyright NSC42Ltd 2020

in <u>https://uk.linkedin.com/in/fracipo</u>

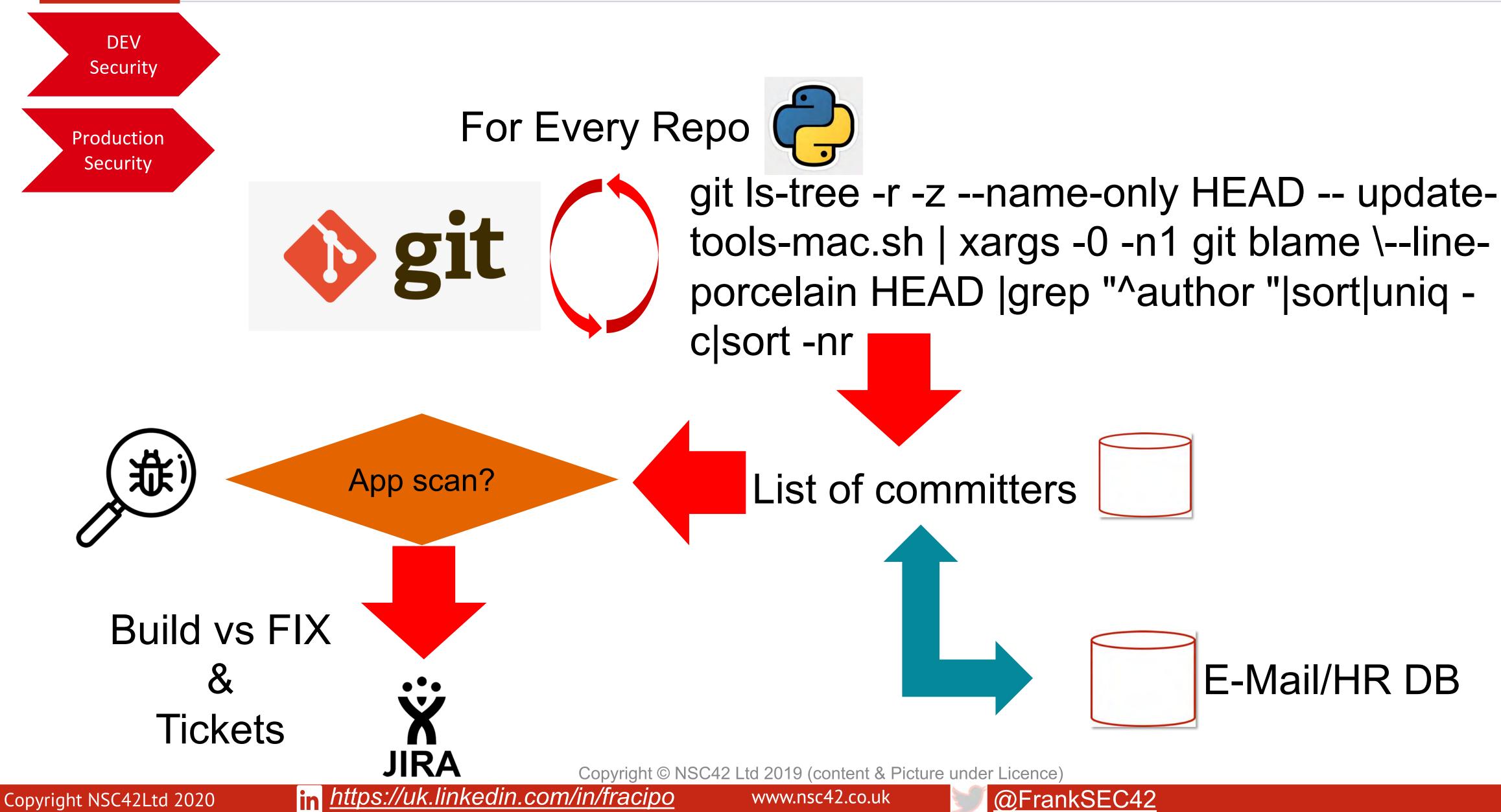


Copyright © NSC42 Ltd 2019 (content & Picture under Licence)





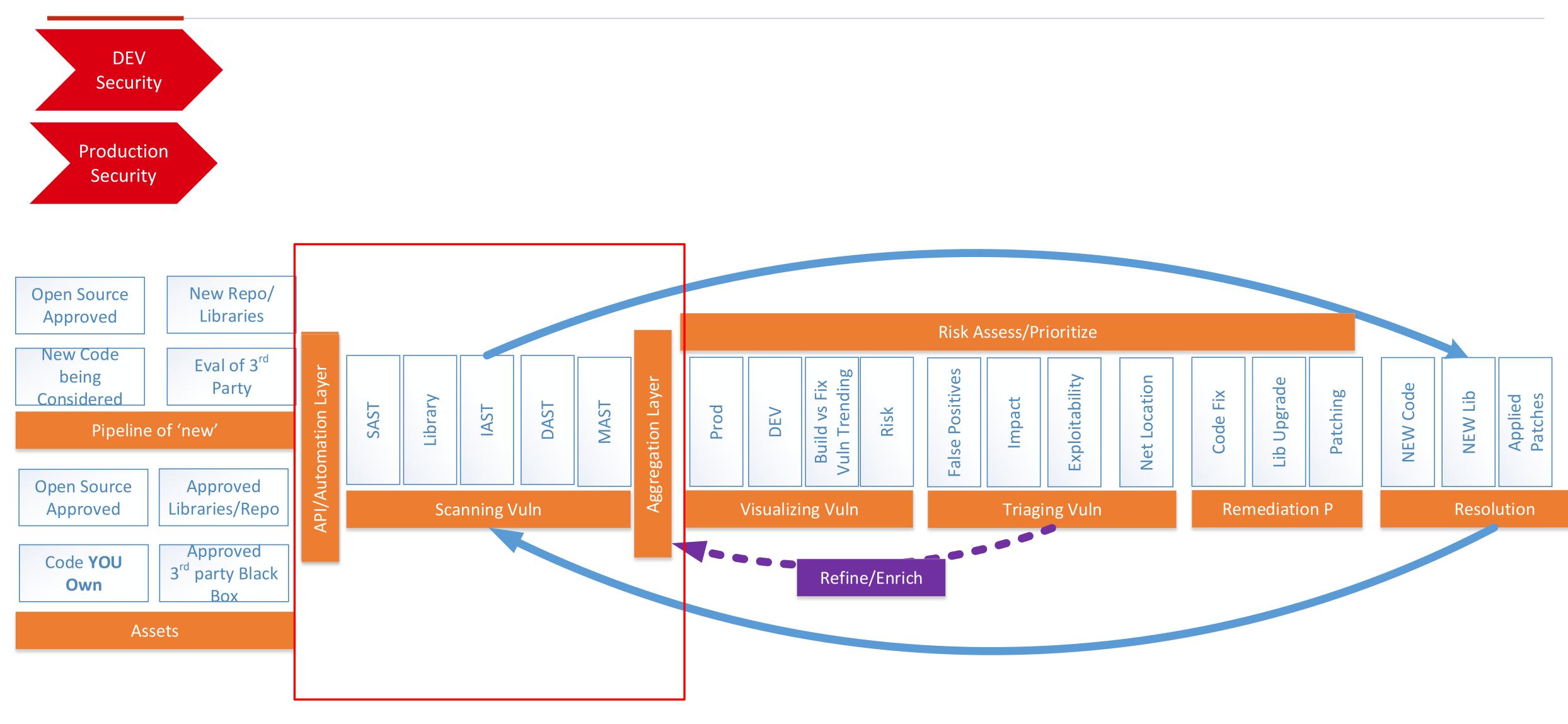
Git to People: Who does what where Visualizer







Dashboard for Code Defects – Part B



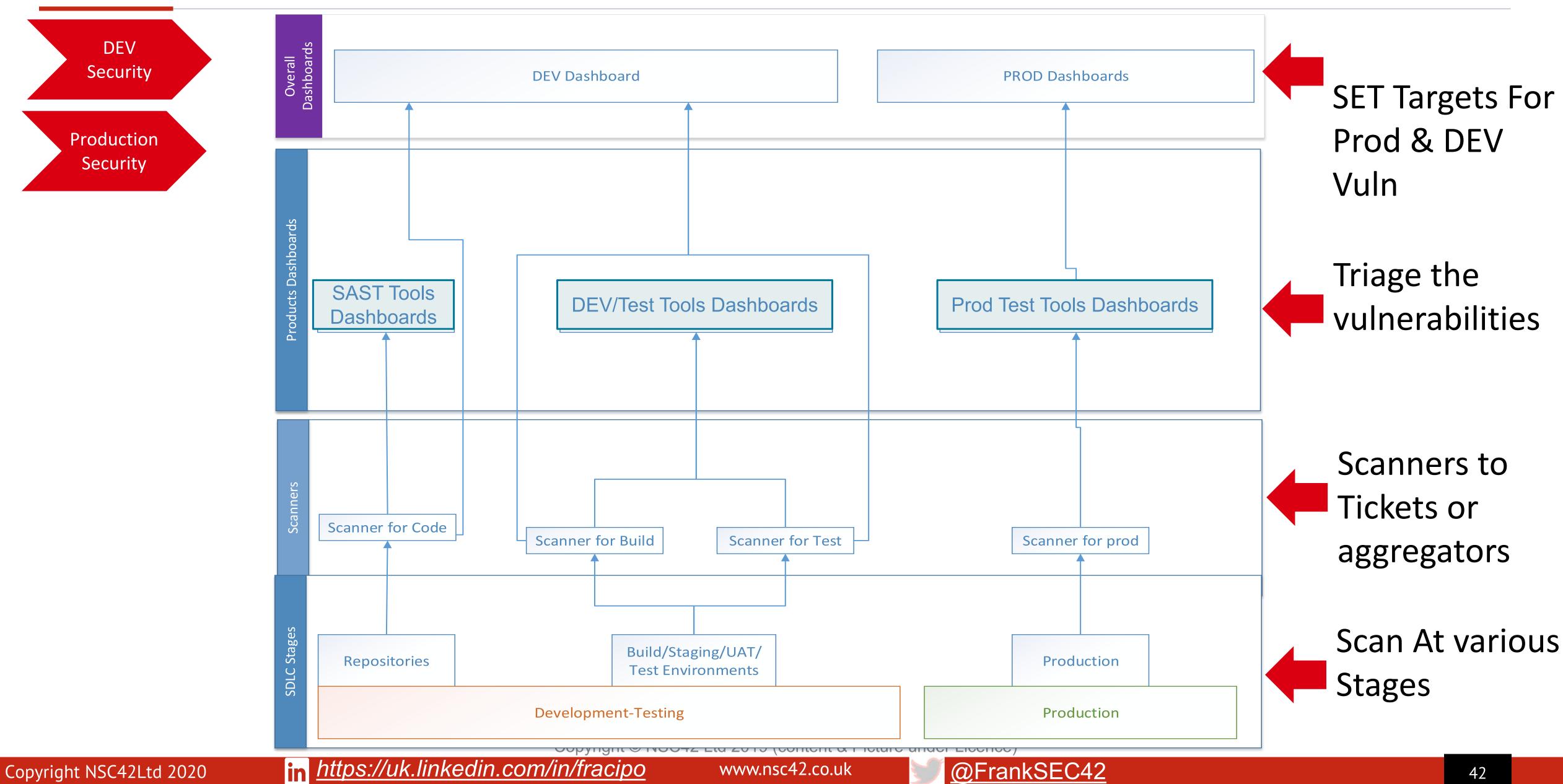
Copyright © NSC42 Ltd 2019 (content & Picture under Licence)

Copyright NSC42Ltd 2020





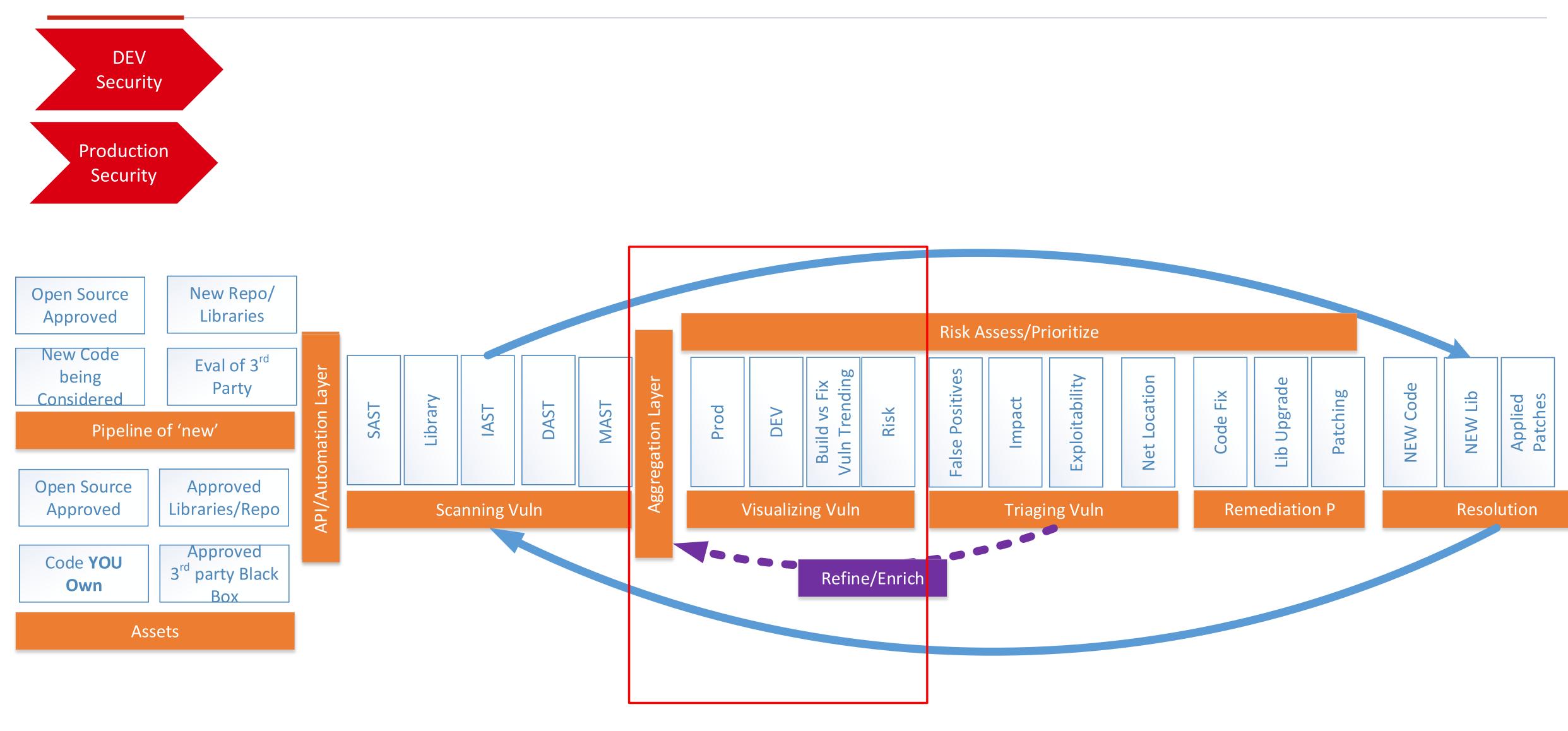
Dashboard for Code Defects -> Under the hood







Dashboard for Code Defects – Part C



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

Copyright NSC42Ltd 2020

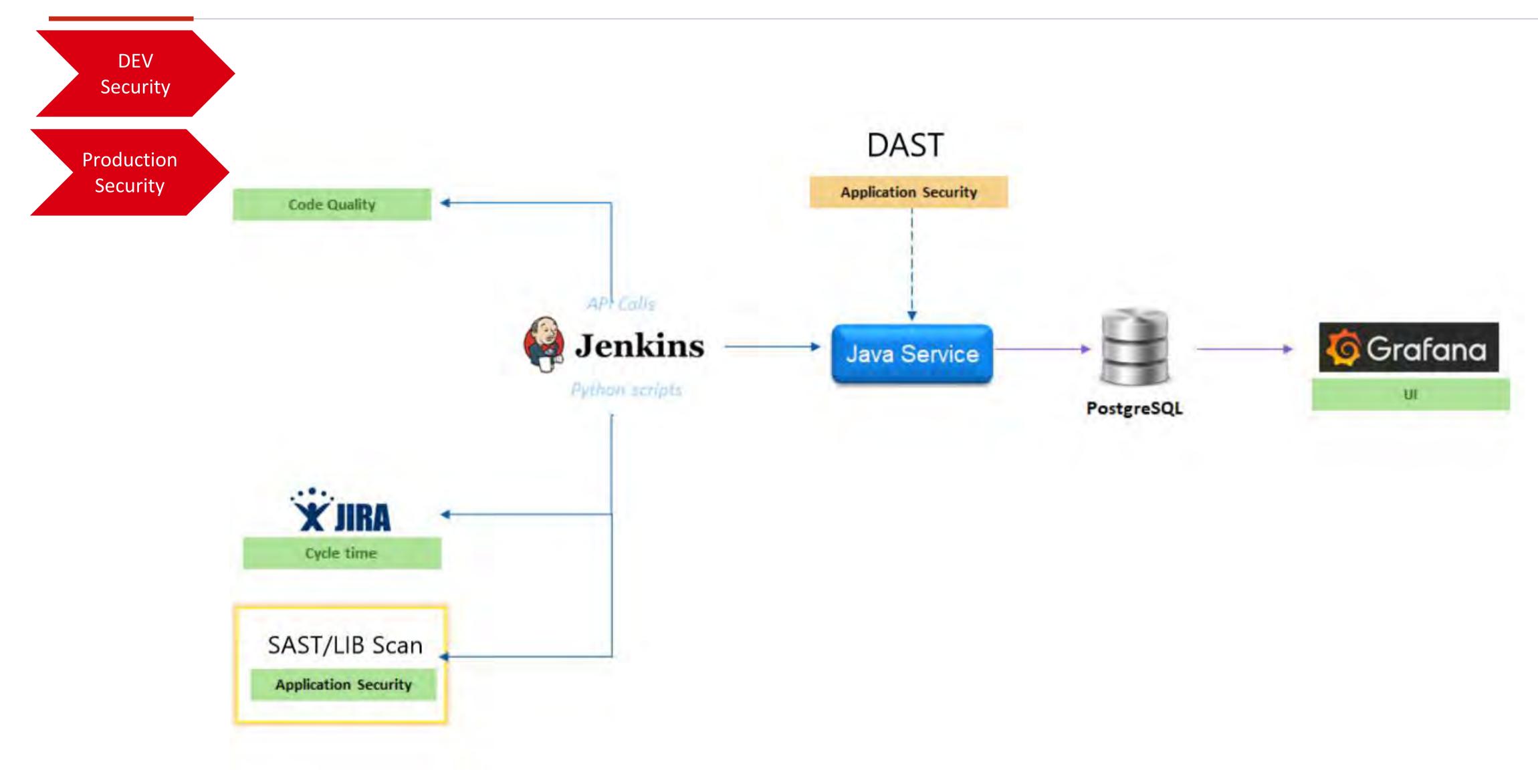








Dashboard for Code Defects



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

Copyright NSC42Ltd 2020

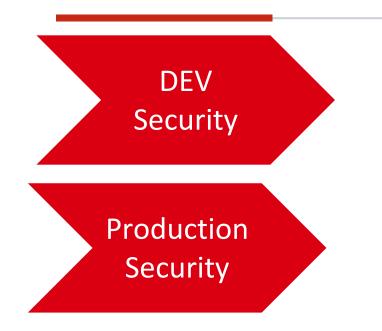




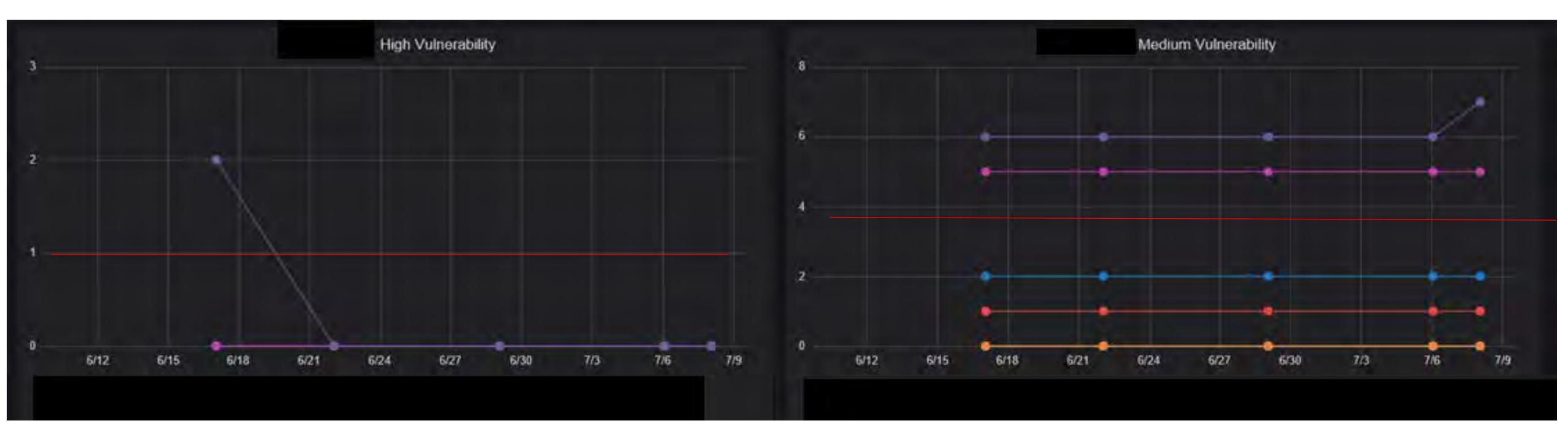




Dashboard for Code Defects



Example of a dashboard for Vulnerability Visualization



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

Copyright NSC42Ltd 2020



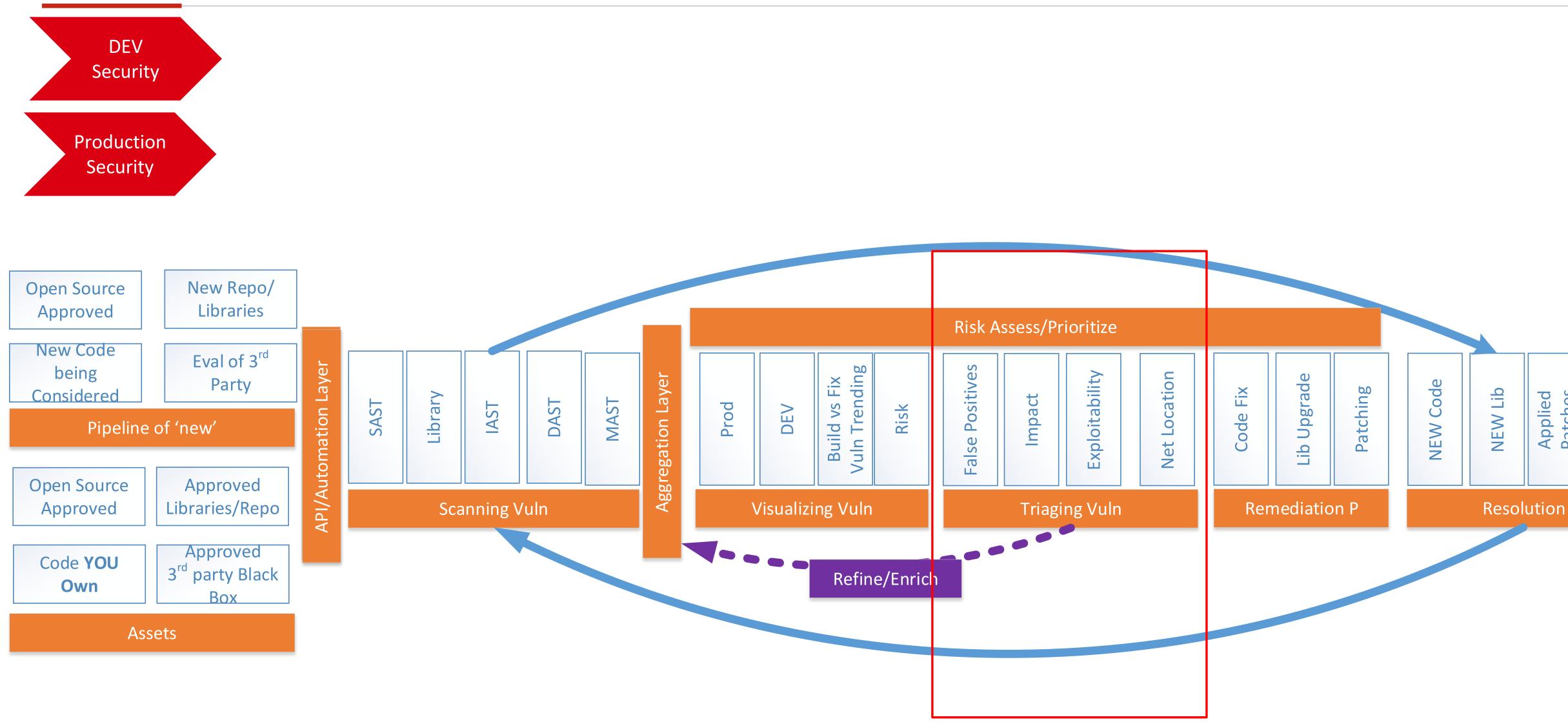


@FrankSEC42





Dashboard for Code Defects - Part D fix



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

Copyright NSC42Ltd 2020

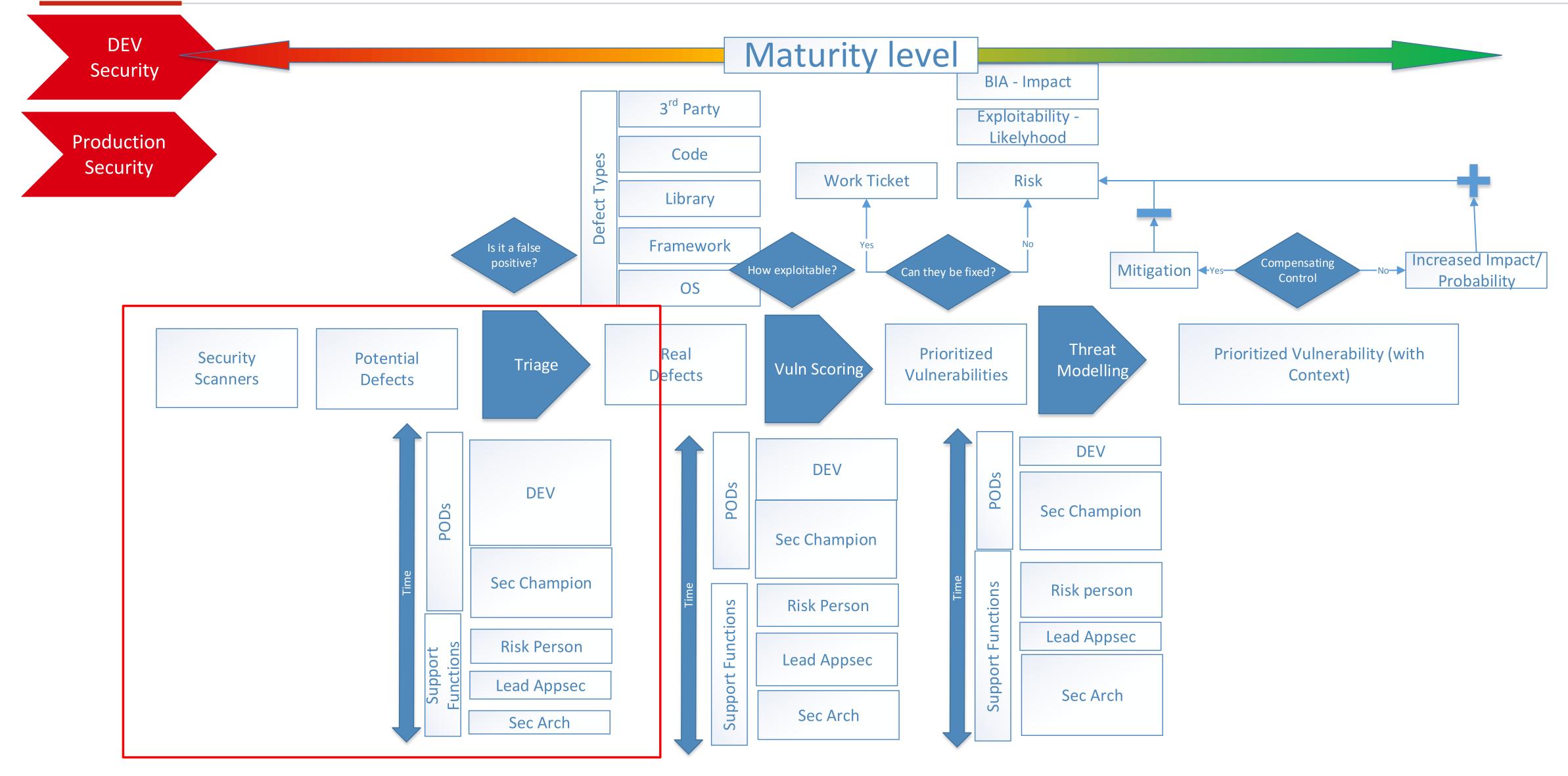








Triaging Vulnerabilities



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

Copyright NSC42Ltd 2020

in <u>https://uk.linkedin.com/in/fracipo</u>



@FrankSEC42

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

in <u>https://uk.linkedin.com/in/fracipo</u>

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

Copyright NSC42Ltd 2020













Trust & Verify Core – Fast & Confident – Core Concepts

Going fast but with confidence (SEC)

1. Trust & Verify

2. License to operate/code

>> Set Thresholds: Bild vs Fix, Vulnerability trending

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

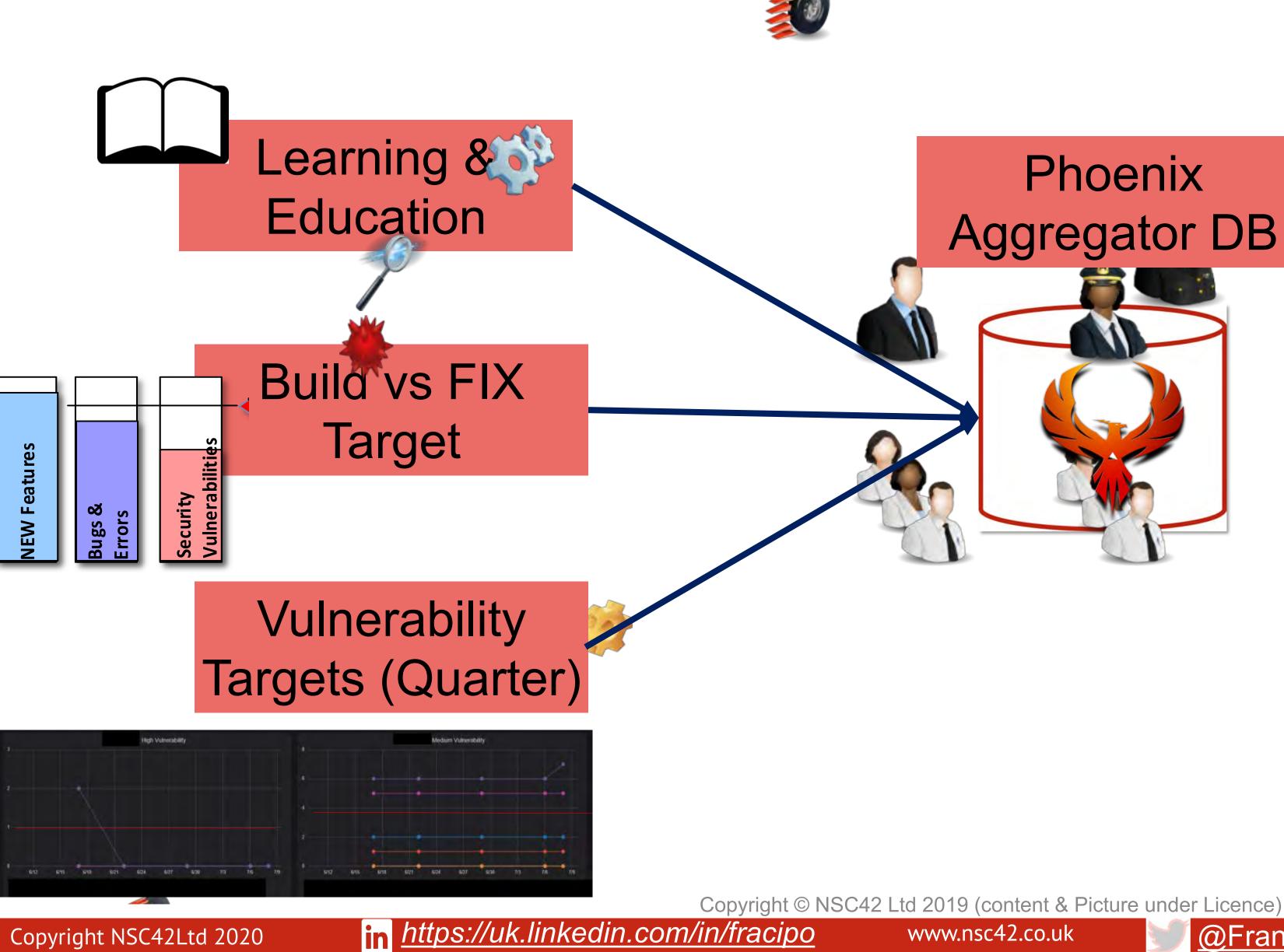


People & Education





Trust & Verify – Under the hood















Security Education in DEV-SEC-OPS



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)



@FrankSEC42



Maturity Model & Recap **Bringing all together**

Copyright NSC42Ltd 2020

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)

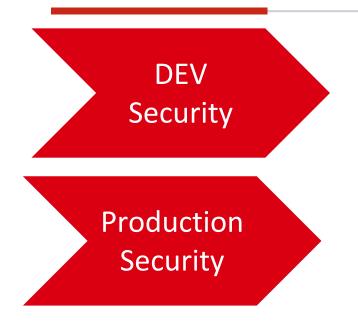
Copyright NSC42Ltd 2020







To Achieve High Maturity what do you do



Overall Maturity

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

Maturity Steps

Mat		How
urity	Task	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	
	No team to pod mapping	
1	No Documentation of Fixes	
	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	
	Adoption Dashboard (advanced) Per A.C. and Per Region	
	Risk Assessment from code scanning with record in Risk management	
	Register	
	Automated Licence to operate: Code Scanning, Libraries, Internal	
3	Training	
4	Fix time of vulnerabilities recorded	
4	T-Shirt Sizing of fixes and Adaptation of SLA based on fixes	
	Visualization of pod to fix	
	segmentation dev and prod	
4	Fix ticket in Jira & Build vs Fix Concept	
4	Fuzzing (basic with generic per app)	
	Automated Licence to operate: Code Scanning, Libraries, Internal	
	Training, Build Vs Fix	
5	Automated Fuzzing & Library of tests Copyright © NSC42 Ltd 2019 (content & Picture	L e unde
	<i>m/in/fracipo</i> www.nsc42.co.uk	

Copyright NSC42Ltd 2020



KCI

			Reporting Frequency
	KCI Mat rutiy	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

Fr Licence)



Fixing Vulnerability the ABC...D



Software you build (repositories)

Vulnerability Data Lake

Select Team Leads and identify security champions

KPI Reporting & Dashboard

Reporting Dashboards (based on the maturity & KPI)

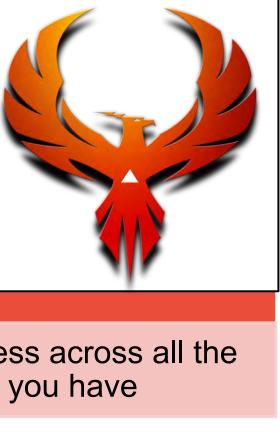
Prioritizing & Vulnerability Reduction

7 – Schedule Vuln Fixes (Jira)

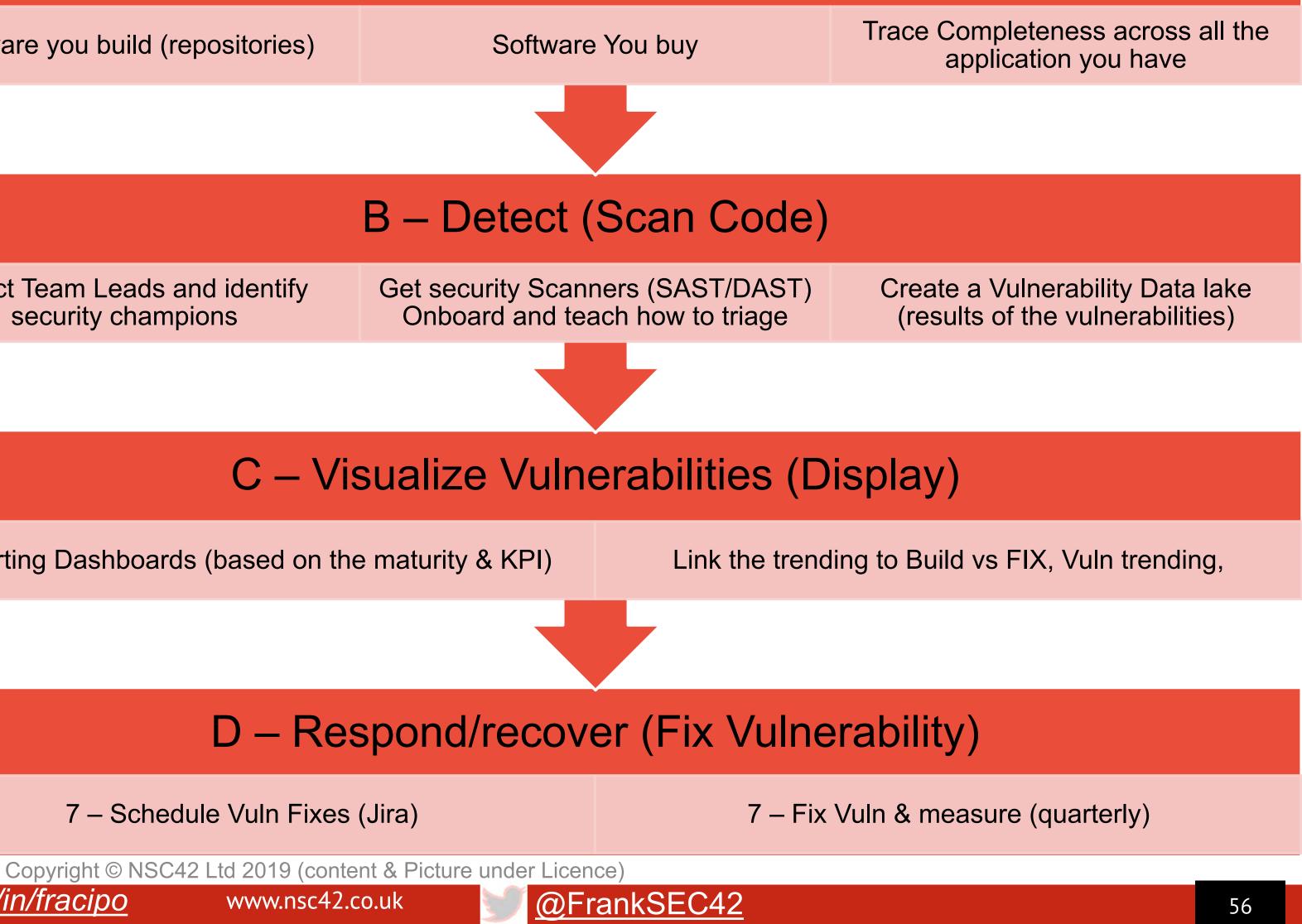
Copyright NSC42Ltd 2020

in <u>https://uk.linkedin.com/in/fracipo</u>





A - IDentify (Software Asset Register)







Conclusion

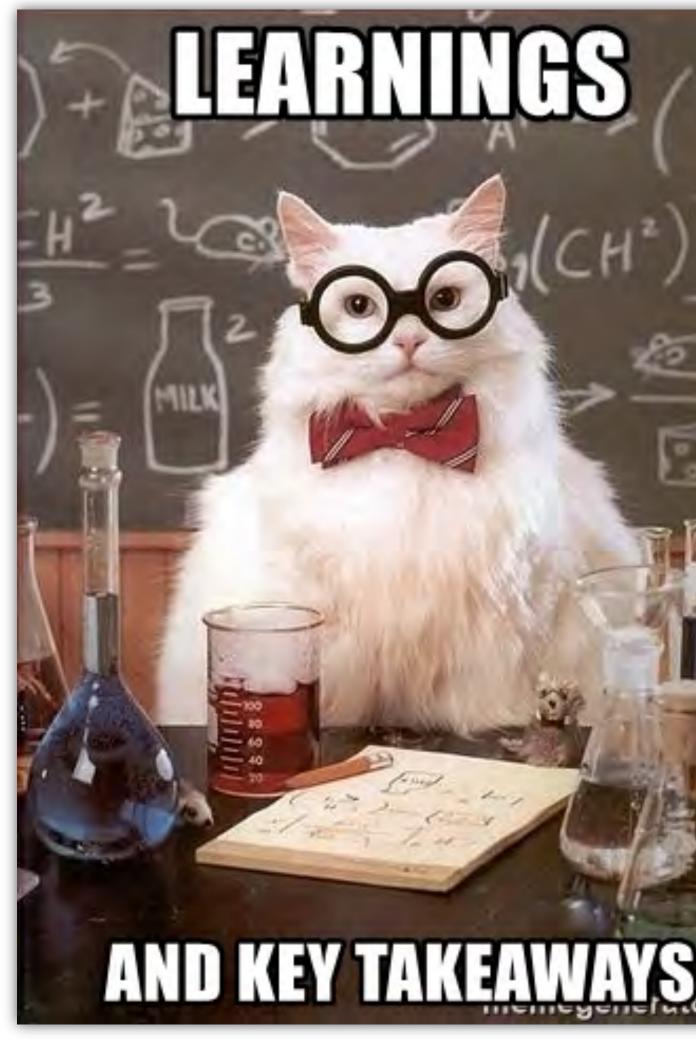
Security is everybody's job **DEV and OPS?**

- 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)

Copyright NSC42Ltd 2020









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 costeffective for your organization's risks appetite.



We offer a range of products within cybersecurity.



VCISO/INTERIM CISO



CYBER SECURITY STRATEGY



CYBER SECURITY CONSULTANCY



@FrankSEC42







Contacts

NSC42

Thank you Get in touch:



https://www.linkedin.com/company/n sc42-limited



Communications@nsc42.co.uk

www.nsc42.co.uk

Copyright © NSC42 Ltd 2019



WHEN YOU ARE CYBERSAFE WE ARE CYBERHAPPY



Cyber Security & Cloud Podcast

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

www.nsc42.co.uk/cscp





Sponsored By

<u>@podcast</u> cyber CorrankSEC42 www.cybercloudpodcast.com





Cyber #MentoringMonday Podcast

Every 2 weeks 1.30 PM UK Time









FFICIA

(ISC



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



Q&A



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

Copyright NSC42Ltd 2020







Contacts

NSC42WHEN 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)





