Damn SMART Cloud Security

Leveraging the use of Cloud Design, Paved Roads, and Vulnerability management for a scaled cloud security programme

CSAUK cloud security alliance SM
UNITED KINGDOM Chapter

APPSEC PHOENIX

SMART Cloud & Software Security

Francesco Cipollone, Founder & CEO
fc@appsecphoenix.com

About Francesco

Francesco Cipollone

Founder AppSec Phoenix, 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

Security Is everyone's job … so better do it DAMN SMART

Security needs automation and scale … paved roads & proactive controls

Warning

Our Agenda

The Landscape

The Problem

The Patterns

Dev/Sec/Ops & Vuln management

Stages of Devsecops & CloudSec

Take Away

Q&A

Setting the Scene

Cloud Evolution – Cloud is not new

SaaS Abstraction & more abstraction

2005 Datacentre Land

2006 amazon.com web services

2007

2008 Google app engine, vmware, rackspace hosting

2010 Microsoft Azure, IBM Cloud

2011 IBMSmartCloud

2012

2013 Google Compute Engine

2014 **Cloud Adoption**

Major Breaches

Why security is everybody's responsibility?

Because we all get affected by it…

2009/
2010
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
Myspace
Twitter
Yahoo

2018
Marriot
Twitter
MyHeritage
Uber
Quora..

2020
Microsoft
Este Lauder
Whisper
MGM
Warner Media

Why Cloud and Why Security

Total cost of cloud breaches

5 trillion $ / 4 trillion GBP

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

N. Of Vuln records

33 billion

Disclosed records over 1 year

Data breaches

10% data breach because of misconfiguration

Cloud misconfiguration is dominat

Av. Cost per record

150$ per record

Average cost per loss record

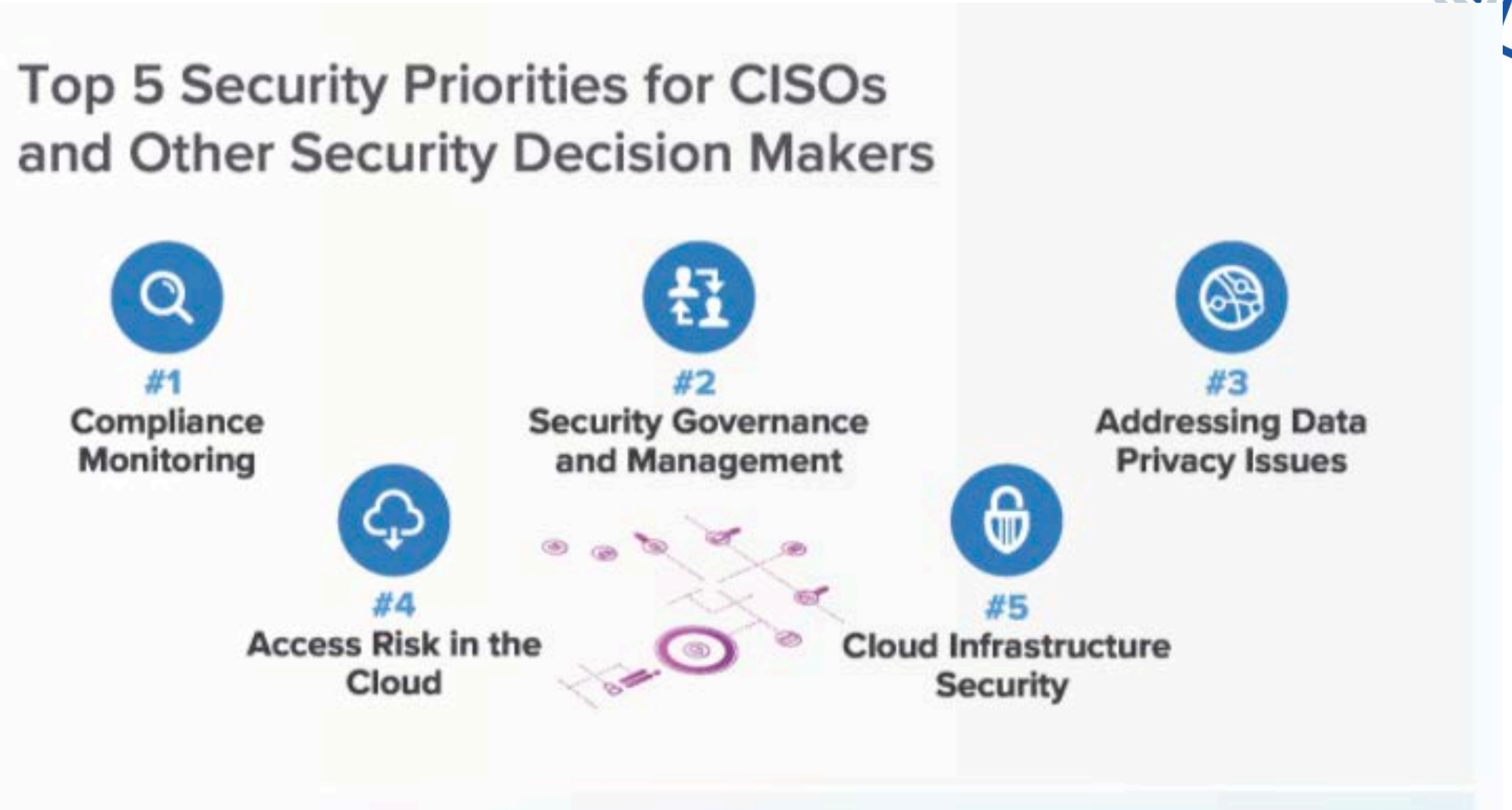
Some of the concern we face today (IDG)

Concerns

- Cloud Misconfiguration
- Lack of Visibility

Priorities

- Compliance and Cloud Monitoring
- Authorization & Authentication
- Security Configuration management



Top 5 Security Priorities for CISOs and Other Security Decision Makers

#1
Compliance Monitoring
#2
Security Governance and Management
#3
Addressing Data Privacy Issues
#4
Access Risk in the Cloud
#5
Cloud Infrastructure Security

https://ermetic.com/resources/infographics/idc-infographic-identity-first-cloud-security-is-essential/

When we are here…we are reactive

We need more proactive controls

Top Cyber Security Risks – CSA Report

1. Data Breaches

Credential Loss & detection

e.g. Sony

2. Misconfiguration & Change Control

Assets Configured incorrectly e.g. S3 Bucket Open

3. Lack of Cloud Security Arch

Contextual View could leave door open e.g. Use of public Storage for private data

4. Broken Access Control

Understanding IAM Roles.

Keys not in Code

5. Account Hijack

Access to Cloud master account

6. Insider Threat

Rogue Admin,

Rogue Collaborators inside

Bribable individuals

7. Insecure API

CSA Api secure,

Key to access the API must be secured

8. Weak Control Plane

Multi Cloud

Control for data migration (CI/CD)

9. CSP API Usage

Immature CSP don't provide mechanism to access services via API

10. Poor Cloud Usage Visibility

Lack of monitoring means inability of detection of misuse

11. Abuse of Cloud Services

Increase of usage

Usage in unmonitored regions

Top Threats to Cloud Computing
The Egregious 11

https://cloudsecurityalliance.org/press-releases/2019/08/09/csa-releases-new-research-top-threats-to-cloud-computing-egregious-eleven/

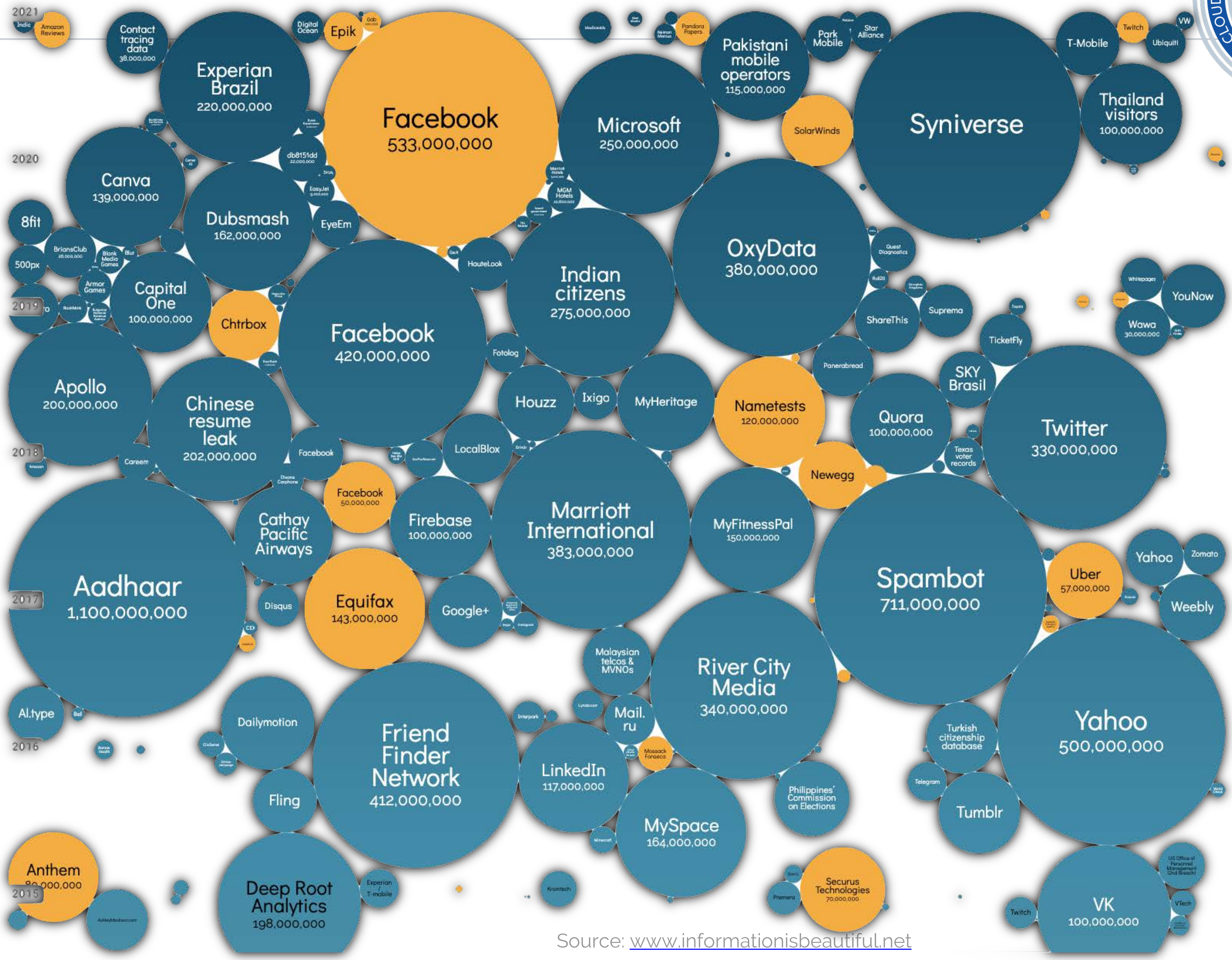
Why security?

CLOUD SECURITY ALLIANCE OFFICIAL CHAPTER United Kingdom Chapter CSA

Data breaches exposed 4.1 billion records in the first half of 2019.

Data breaches are the new norm. They threaten the viability of every business as they're now larger in number and impact.

it takes only one misconfiguration to get a you in front of the newspaper



Source: www.informationisbeautiful.net

https://appsecphoenix.com/6-biggest-cybersecurity-breaches-of-last-decade-shocking-cybersecurity-stats-2/

Can we solve this problem just with Bodies?

More deployment every day, more features, more automation

2015

Dev Ops Sec

100 : 10 : 1

Sec Apps

1 : 10

2020

Dev Ops Sec

750 : 75 : 1

Looks Like we have a scale problem

Can we solve this problem just with Bodies?

Can we solve this problem just with Bodies?

How do we do it

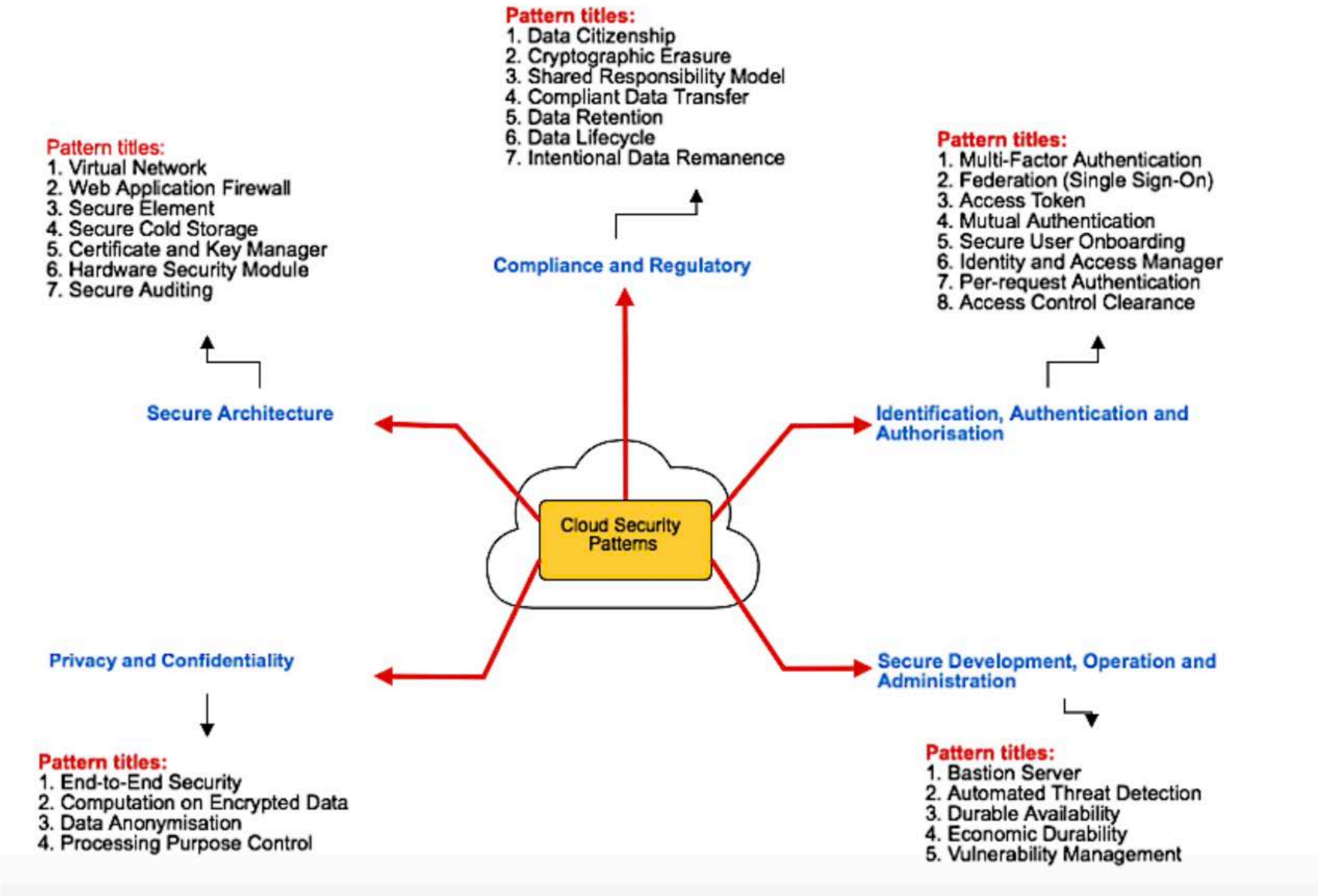
- **Guardrails**
- **Baselines**
- **Defining how environment looks like**

Security Pattern? Why?

How do we do it

- **Define it once**
- **Use it many Times**

- **Define use cases that are more common and patternize them**



Cloud Security Patterns

Compliance and Regulatory

Pattern titles:
1. Data Citizenship
2. Cryptographic Erasure
3. Shared Responsibility Model
4. Compliant Data Transfer
5. Data Retention
6. Data Lifecycle
7. Intentional Data Remanence

Secure Architecture

Pattern titles:
1. Virtual Network
2. Web Application Firewall
3. Secure Element
4. Secure Cold Storage
5. Certificate and Key Manager
6. Hardware Security Module
7. Secure Auditing

Identification, Authentication and Authorisation

Pattern titles:
1. Multi-Factor Authentication
2. Federation (Single Sign-On)
3. Access Token
4. Mutual Authentication
5. Secure User Onboarding
6. Identity and Access Manager
7. Per-request Authentication
8. Access Control Clearance

Privacy and Confidentiality

Pattern titles:
1. End-to-End Security
2. Computation on Encrypted Data
3. Data Anonymisation
4. Processing Purpose Control

Secure Development, Operation and Administration

Pattern titles:
1. Bastion Server
2. Automated Threat Detection
3. Durable Availability
4. Economic Durability
5. Vulnerability Management

https://www.mdpi.com/2073-431X/8/2/34/pdf-vor

So we solved security right

Paving the Road

AppSec Phoenix DevSecOps Framework

SDLC

Security Design

Secure Build/Test

Secure Operate

Define Guardrails

Define Pattern

Enforce & Monitor

Vulnerability management

Red Team/Testing

Vulnerability management

Red Team/Testing

PenTest

Obligation

Standards

Principles

Patterns

Requirement

Security Standards
Security Principles
Security Requirements
Regulations

Design

Secure Design Patterns,
Service Patterns
Security Assessment/Question,
Security Architecture

Development

Secure Coding Practice
Static Code Analysis
FOSS & Library security

Dev Testing

Secure Code Review,
Vulnerability Assessment
Security Test Stories
Threat Model Stories
Dynamic code Analysis

Deployment

Terraform and embedded security
Security Standards
Golden and approved AMI/Gold Repo
Approved Repo
Threat Model

Operational

Vulnerability Visibility
Image Redeployment/Rebuild
Cloud Config Testing

Security Intf

Sec Libraries

Paved Roads

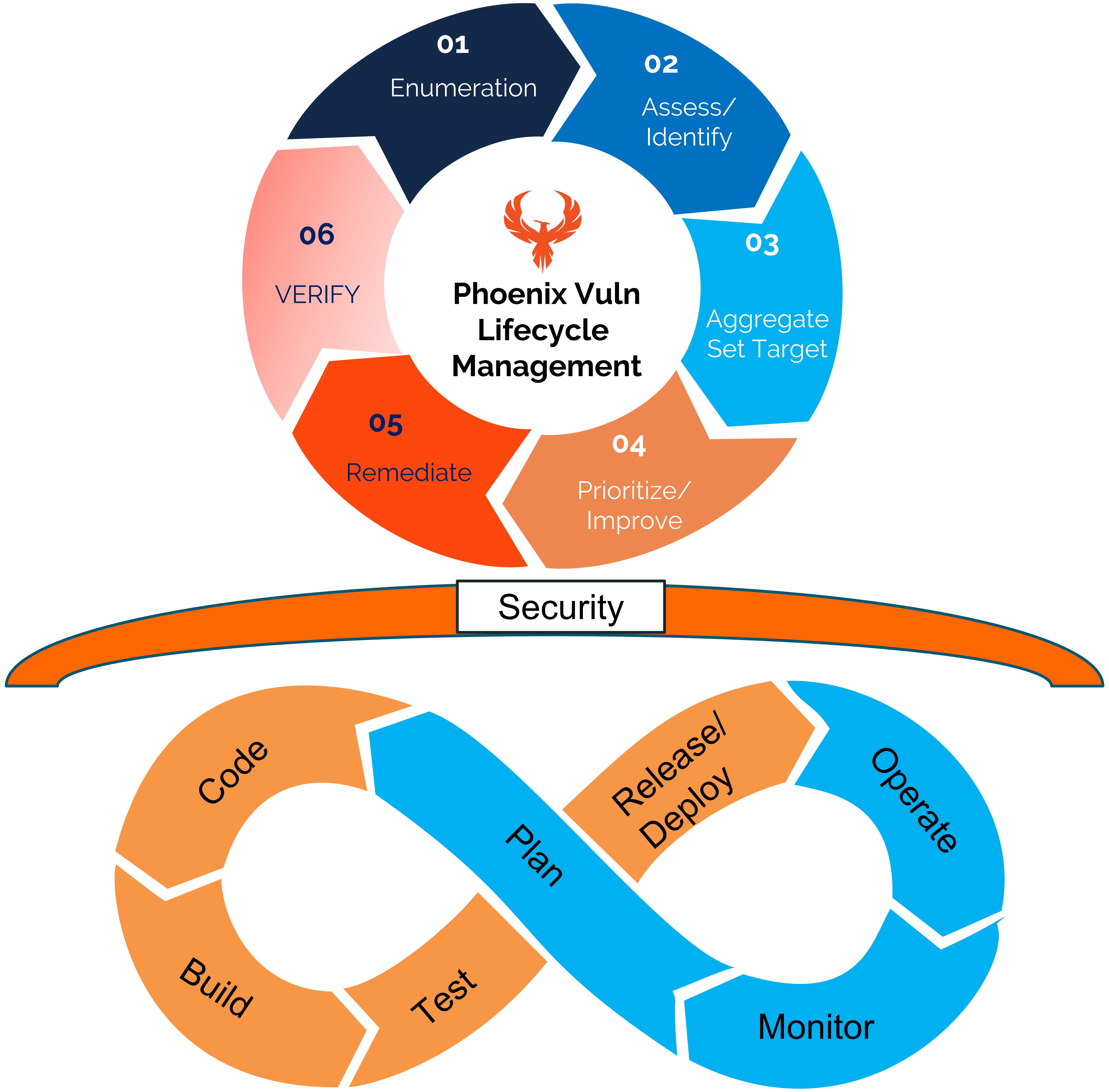
Design & Architecture Vuln Management

Vuln Management in Dev/Test

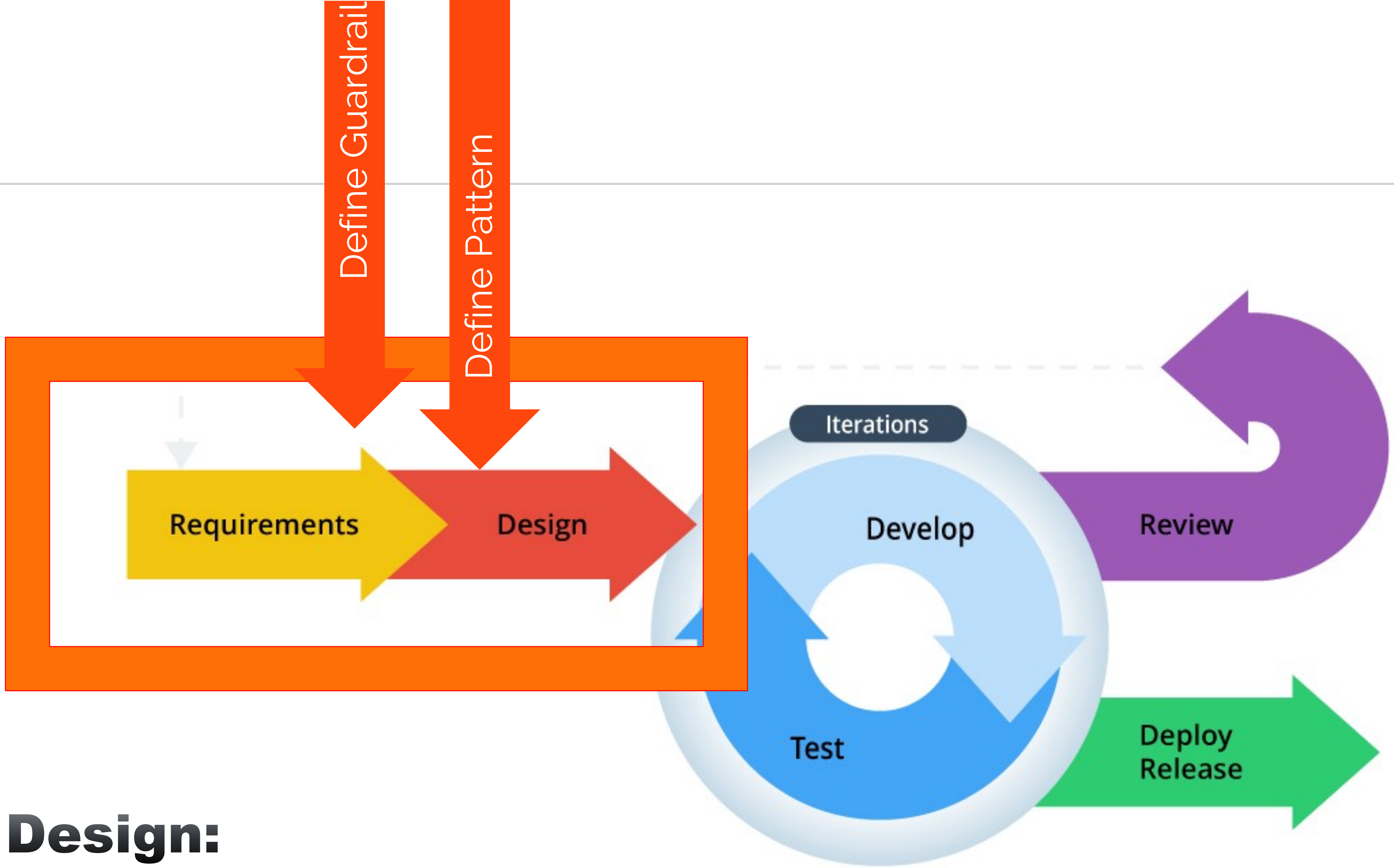
Vuln Management in Live/Ops

So we solved security right

DevOps+SEC Cloud Security Meets Dev Sec Ops



DevSecOps In design

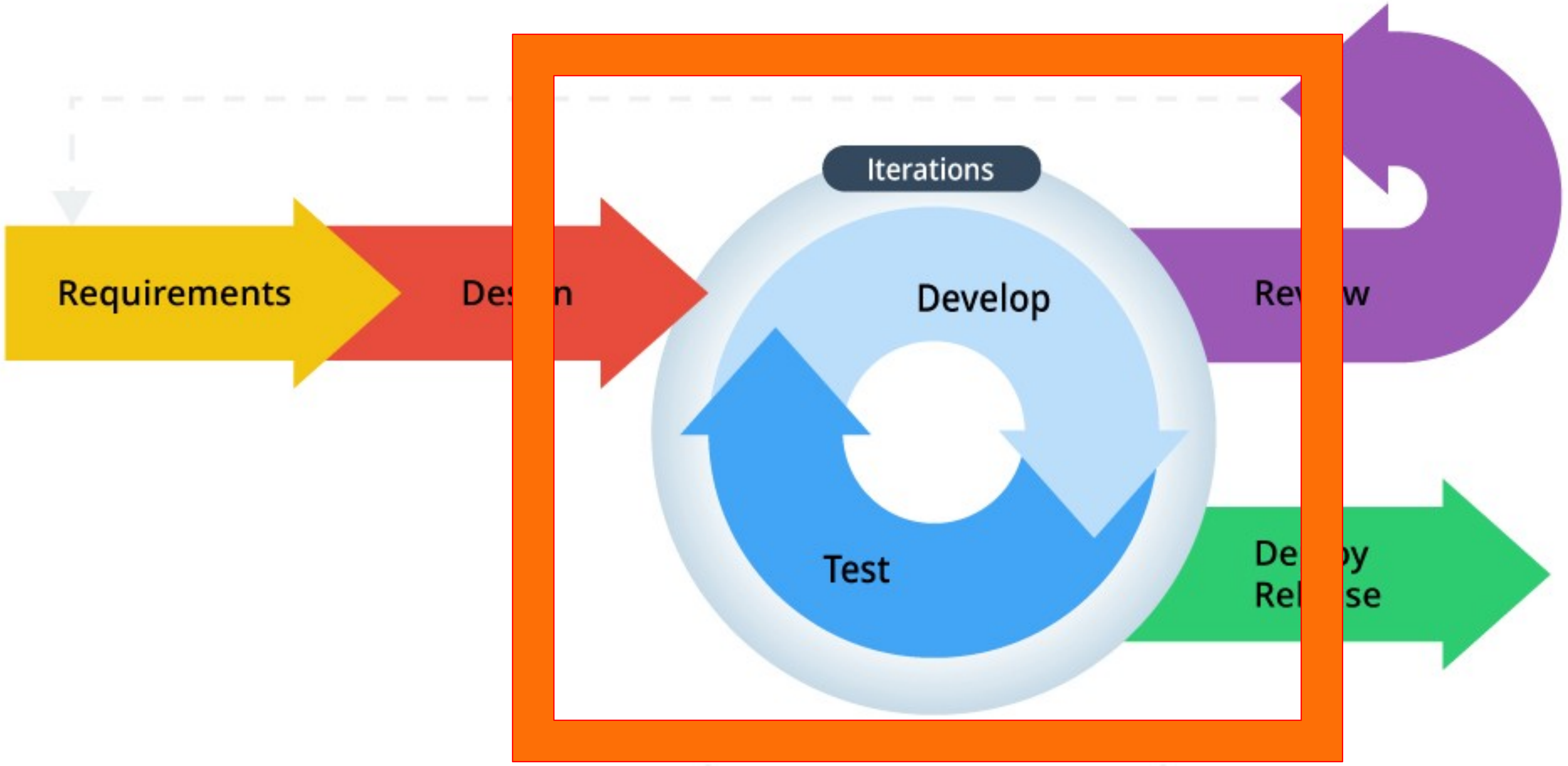


Design:

- **Define Designs**
- **Define Guardrail**
- **Enforce them with**
- **Automate Deployment model**

Keep Working with team to define what can be standardized

Step 6 – Stages

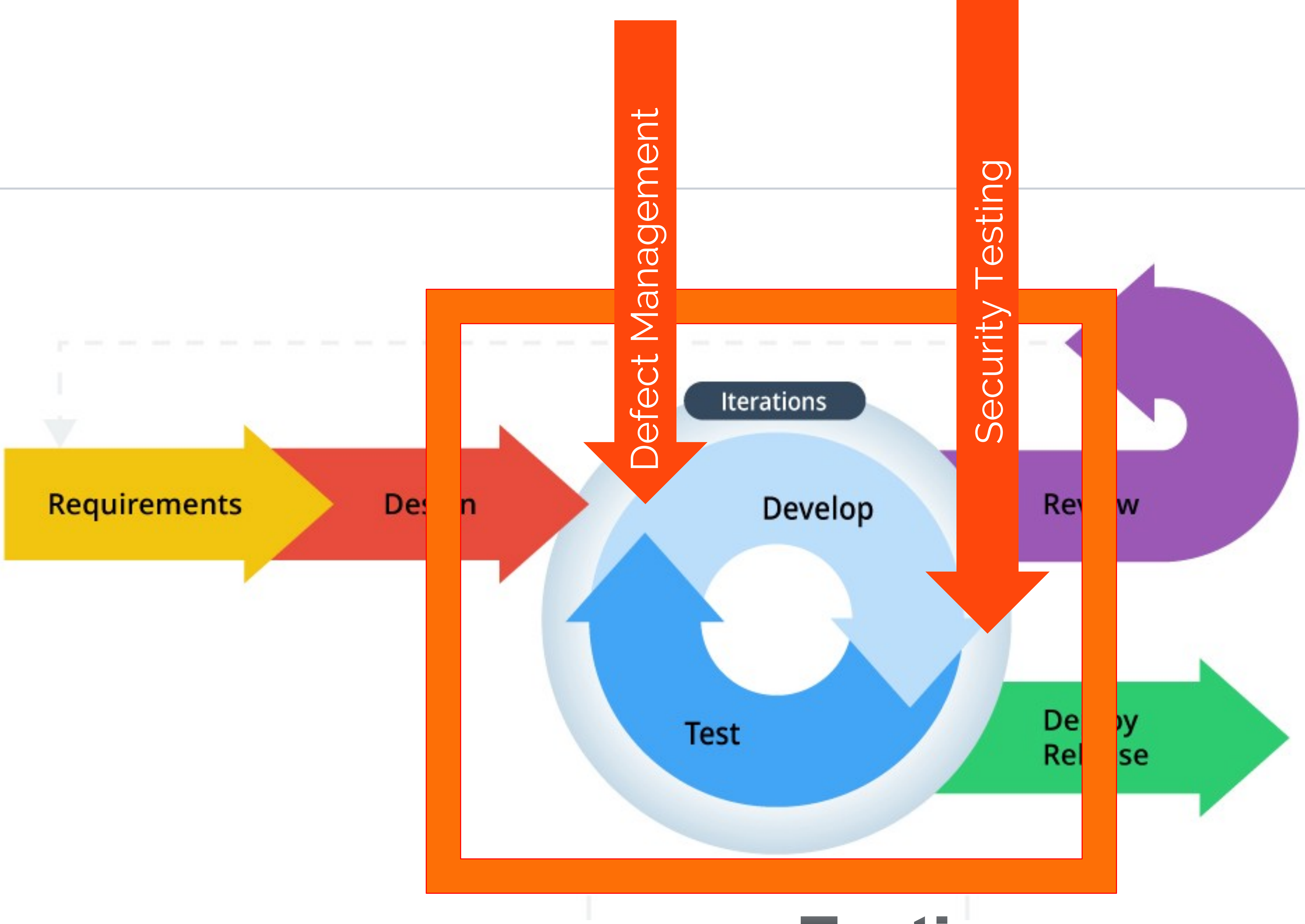


Enforcement

- **Enforce Guardrail**
- **Enforce Patterns**
- **Build Standard**
- **Deployment model**
- **Remove Friction**

Keep Working with team to define what can be standardized

Dev & Test



Prioritize

Testing

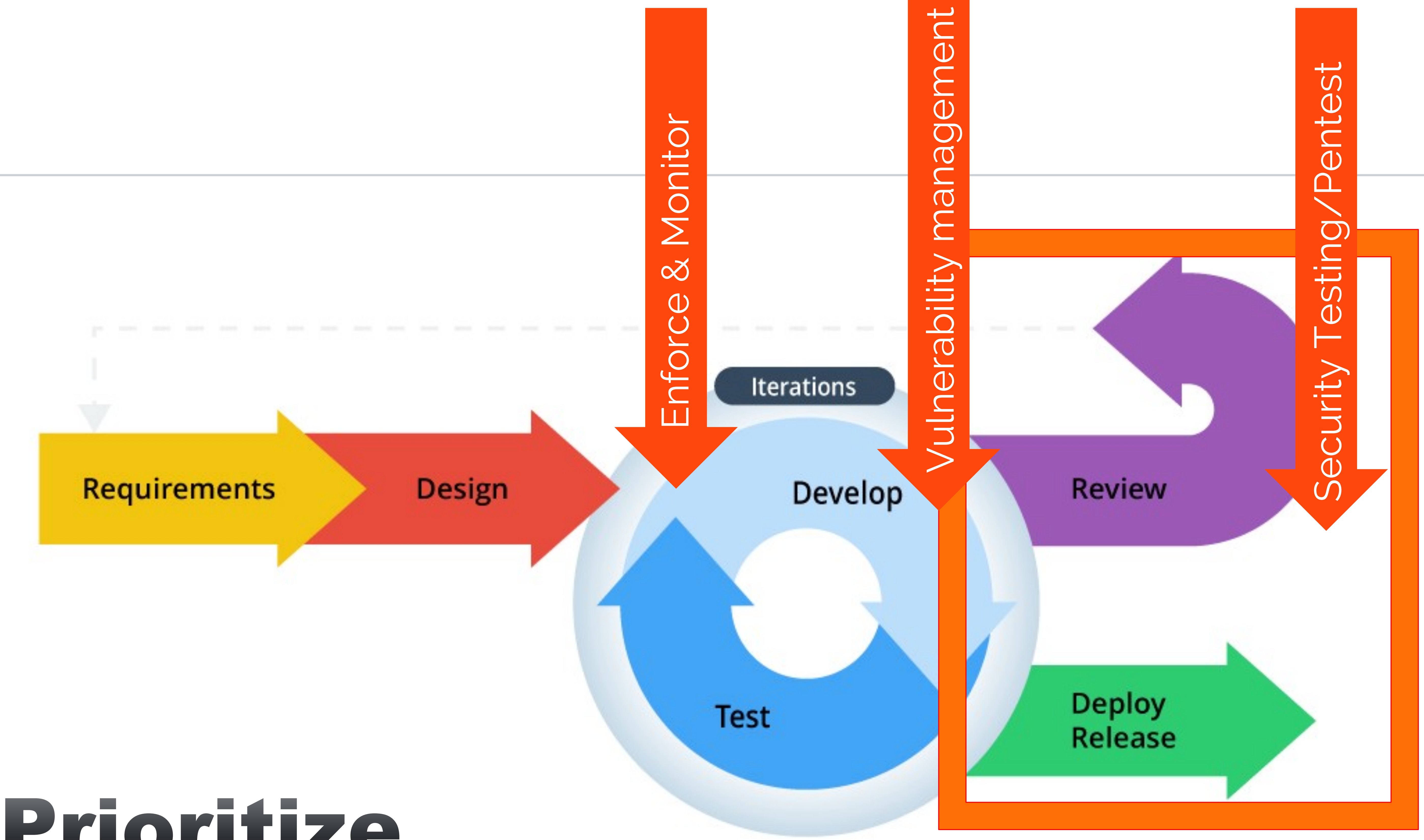
- Automate Testing

- Apply testing standard or rely on predefined rules

- Review Vulnerabilities Prioritize

Keep Working with team to define what can be standardized

Dev & Test



Prioritize

Pentest

- **Pentest Occasional as verification**
- **Red team and CTF**

Prioritize

Security Testing

- **Automate Testing -> things Change**
- **Apply testing standard or rely on predefined rules**
- **Review Vulnerabilities Prioritize**

Keep Working with team to define what can be standardized

Tooling – Open Source Arsenal

Does not need to cost a fortune

*) Enumeration/Reconnaissance
> https://sitereport.netcraft.com/
> https://github.com/rbsec/dnscan
> shodan.io
> domains
> https://github.com/OWASP/Amass

1) Static code analyser - https://github.com/ShiftLeftSecurity/sast-scan

2) SCA - Dependency-Check - https://github.com/jeremylong/DependencyCheck
npm audit

Dep Check Github Action: https://github.com/dependency-check/Dependency-Check_Action

3) Code relationships - https://github.com/crubier/code-to-graph

3) Cloud Assessment - Prowler - https://github.com/toniblyx/prowler
https://github.com/google/tsunami-security-scanner

4) Network assessment - Nettacker - https://github.com/zdresearch/OWASP-Nettacker
> Tsunami - https://github.com/google/tsunami-security-scanner

For the Full List

https://appsecphoenix.com/open-source-arsenal-how-to-improve-your-security-posture/

Tooling – Maturing and how to measure

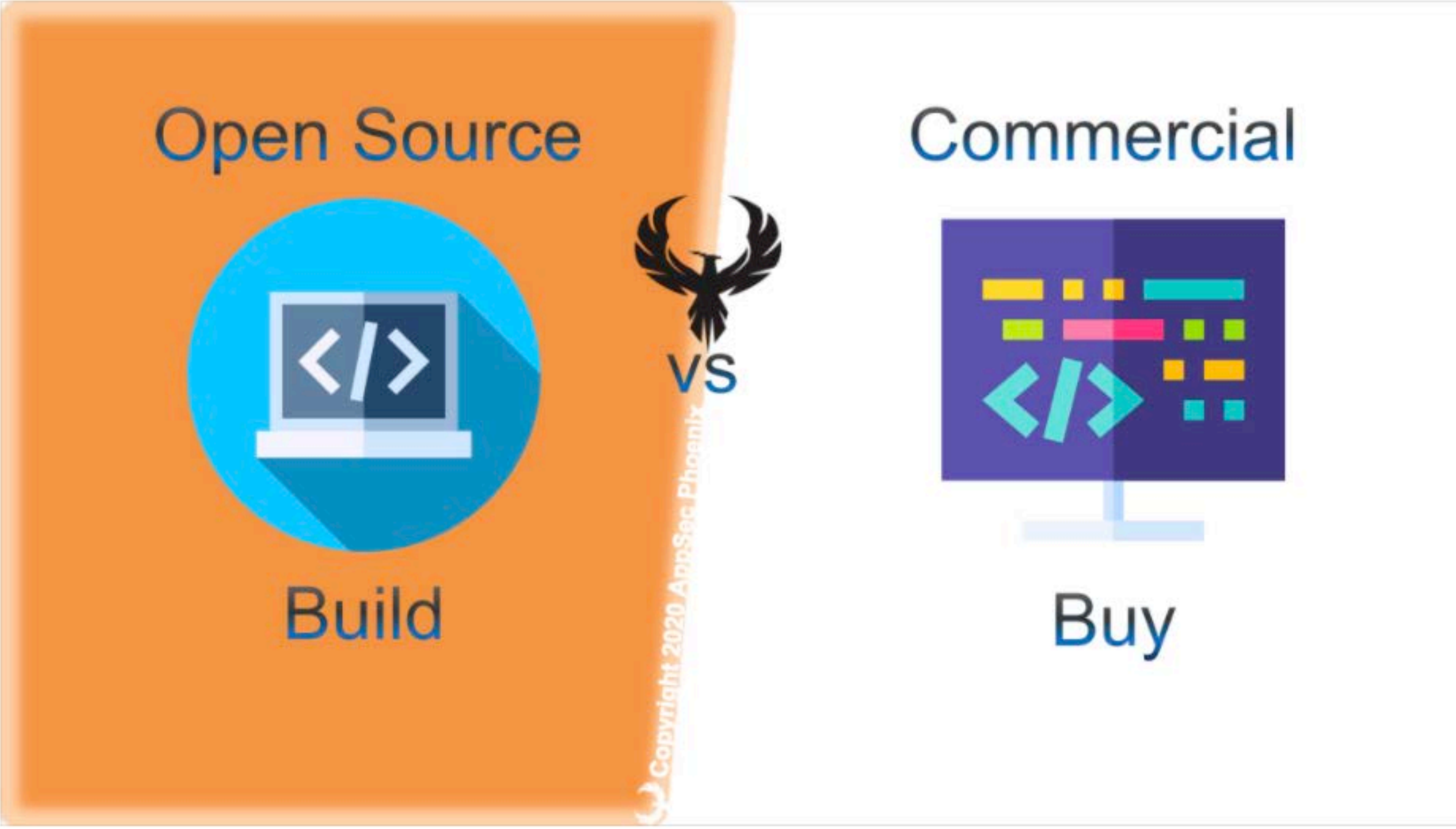
What to look into a scanner

Open source

- Usually affordable or free (open source) but usable
- Available to the whole organization
- Flexible and modifiable

Commercial

- Usable, great user interface
- API and great data extraction
- Pre-created rules
- Pre-created logic
- Lower rate of false positives
- Commercial support
- On demand support/maintenance



For the Full List

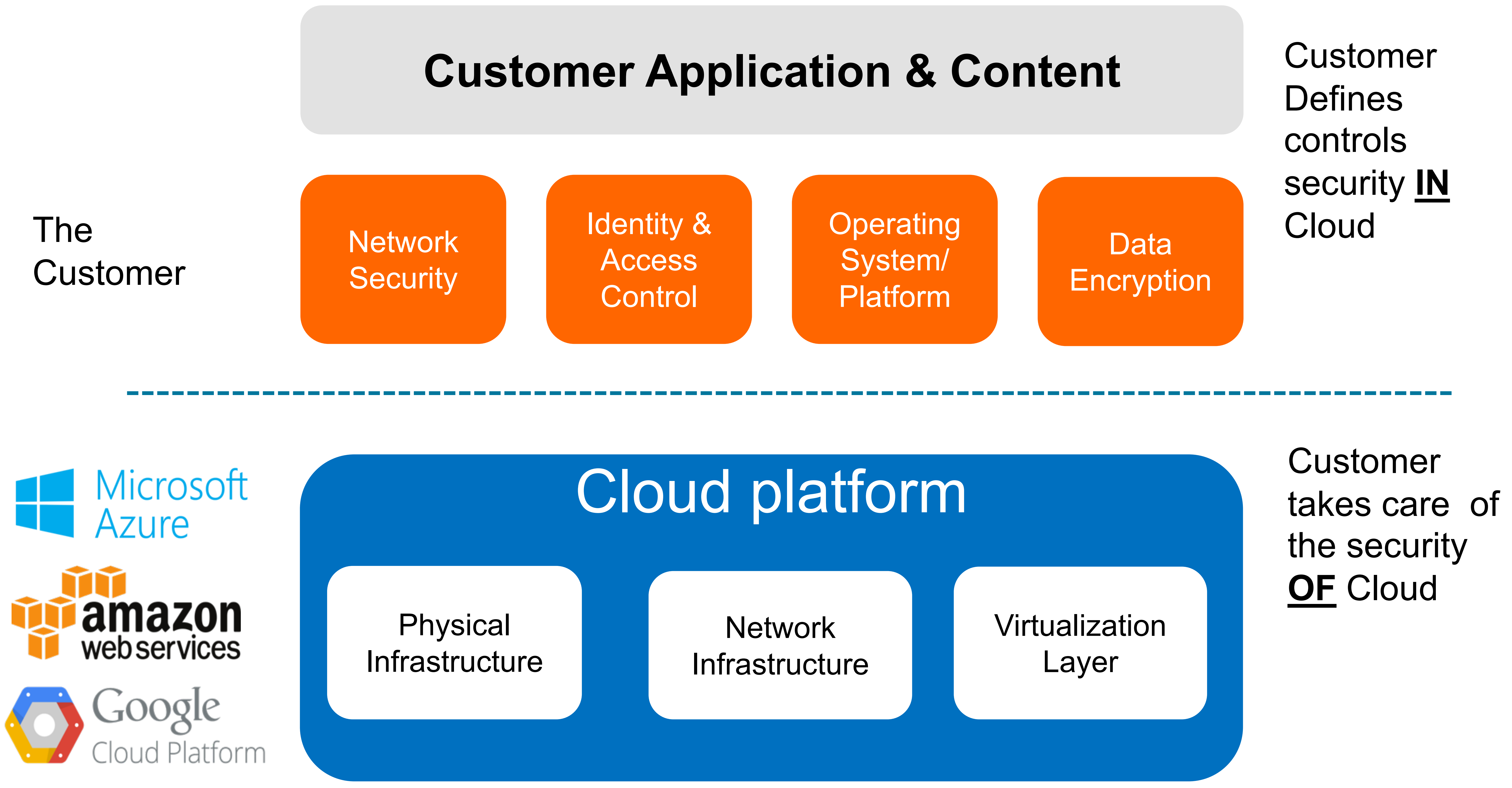
https://appsecphoenix.com/devsecops-open-source-vs-commercial-tools-which-is-best-for-you/

Something More…

Other Aspect to consider – Shared Responsibilities

Consider what are you are getting yourself into in a cloud migration. Cloud is not natively secure or insecure

“Understand Shared Responsibility model Delegation and you’ll master cloud”



Customer Application & Content

The Customer

Network Security

Identity & Access Control

Operating System/ Platform

Data Encryption

Customer Defines controls security **IN** Cloud

Microsoft Azure

amazon web services

Google Cloud Platform

Cloud platform

Physical Infrastructure

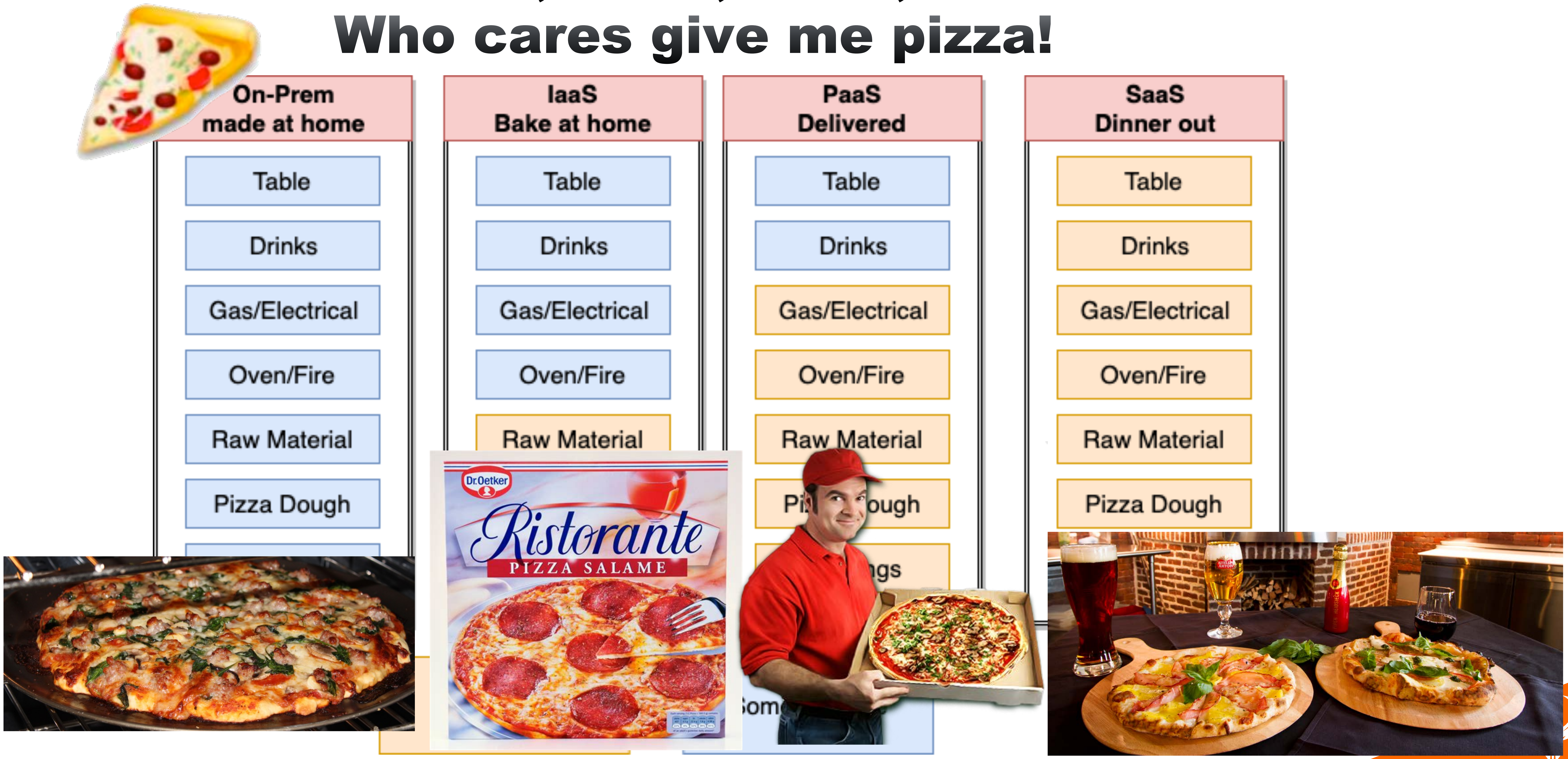
Network Infrastructure

Virtualization Layer

Customer takes care of the security **OF** Cloud

Shared Resp Model

IaaS, PaaS, SaaS, ...
Who cares give me pizza!



On-Prem made at home	IaaS Bake at home	PaaS Delivered	SaaS Dinner out
Table	Table	Table	Table
Drinks	Drinks	Drinks	Drinks
Gas/Electrical	Gas/Electrical	Gas/Electrical	Gas/Electrical
Oven/Fire	Oven/Fire	Oven/Fire	Oven/Fire
Raw Material	Raw Material	Raw Material	Raw Material
Pizza Dough		Pi ough	Pizza Dough
		ngs	
		ome	

CSA Help

Other Tools for foundation

The Six Pillars of DevSecOps
Achieving Reflexive Security Through Integration of Security, Development and Operations
SAFECode
Top Threats to Cloud Computing
The Egregious 11
Cloud Penetration Testing Playbook
Guideline on Effectively Managing Security Service in the Cloud
Top Threats to Cloud Computing: Deep Dive
A case study analysis for 'The Treacherous 12: Top Threats to Cloud Computing' and a relative security industry breach analysis
Best Practices for Implementing a Secure Application Container Architecture
Integrating Application Container Security Considerations into the Engineering of Trustworthy Secure Systems
The 12 Most Critical Risks for Serverless Applications 2019
SECURITY GUIDANCE
For Critical Areas of Focus In Cloud Computing v4.0
CSA cloud security alliance

https://cloudsecurityalliance.org/research/artifacts

Something More...

Conclusions

Wrapping up, we've discussed

- The problem of scalability
- How to be proactive
- Vulnerability management, pattern and automation where do they fit
- We left out so much more

What’s missing

What is missing & what more

- Patterns
- Be proactive and work smart with team -> Talks
- Automate testing as much as possible and PRIORITIZE
- Security Engineering and Paved way: Lesson from Netflix, Robin Hood …

What’s missing

Cloud Security

Paved Roads

- https://www.hella-secure.com/post/create-your-paved-roads
- https://blog.sqreen.com/how-to-use-frameworks-to-implement-your-security-paved-road/
- https://www.slideshare.net/diannemarsh/the-paved-road-at-netflix

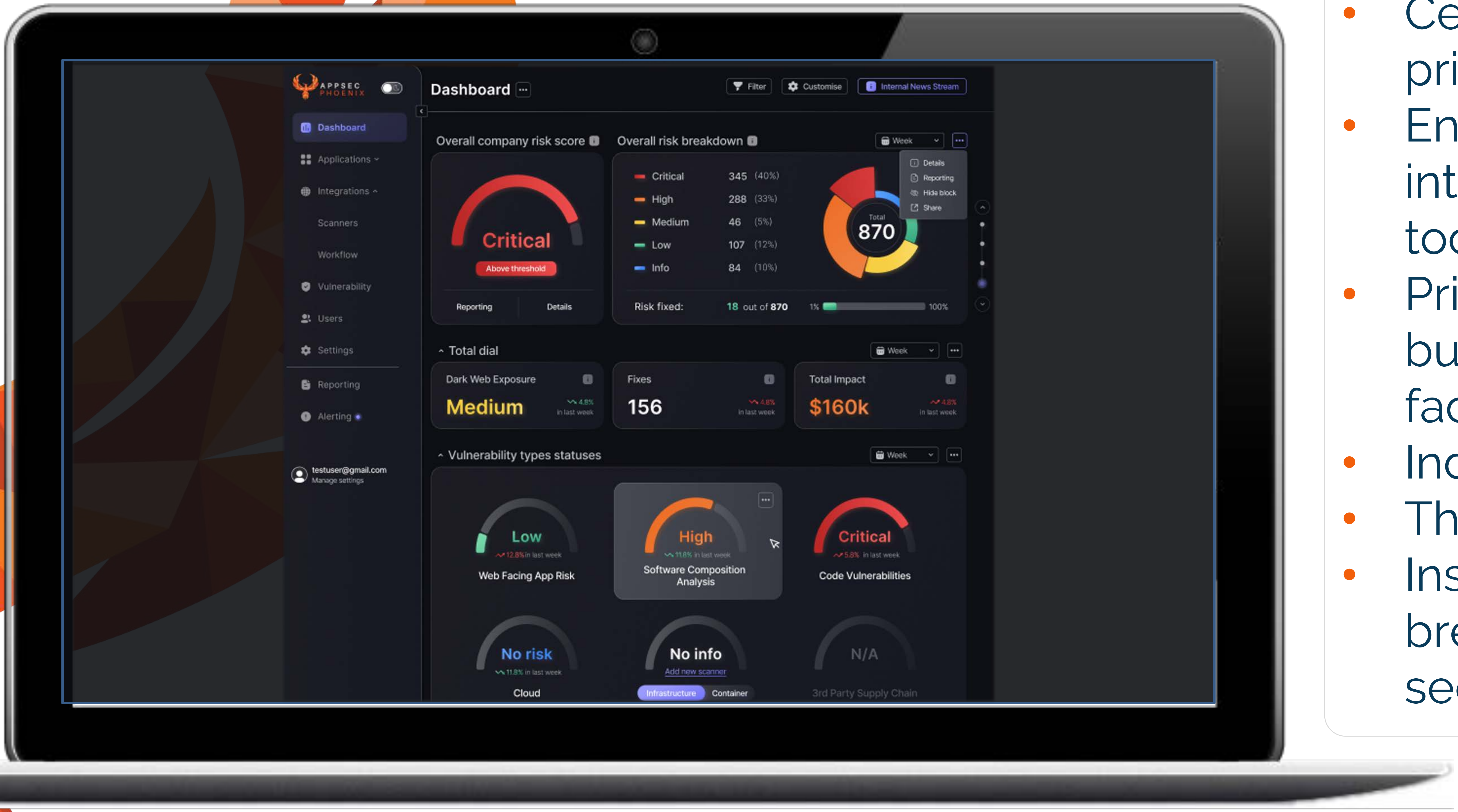
- https://www.researchgate.net/publication/332903539_Security_Pattern_for_Cloud_SaaS_From_System_and_Data_Security_to_Privacy_Case_Study_in_AWS_and_Azure
- http://www.sirris.be.s3-website-eu-west-1.amazonaws.com/
- https://docs.microsoft.com/en-us/azure/architecture/framework/security/security-patterns

Q&A

ONE DOES NOT SIMPLY
GIVE A PRESENTATION WITHOUT Q&A
imgflip.com

AppSec Phoenix Platform

We aggregate and correlate app, infra, cloud vulnerabilities and correlate it in risk based way.
A centralized platform that aggregates vulnerabilities from cloud, software and enriches them with business insights to provide a prioritized view to developers and single pane of glass to executive on the risk of their enterprise

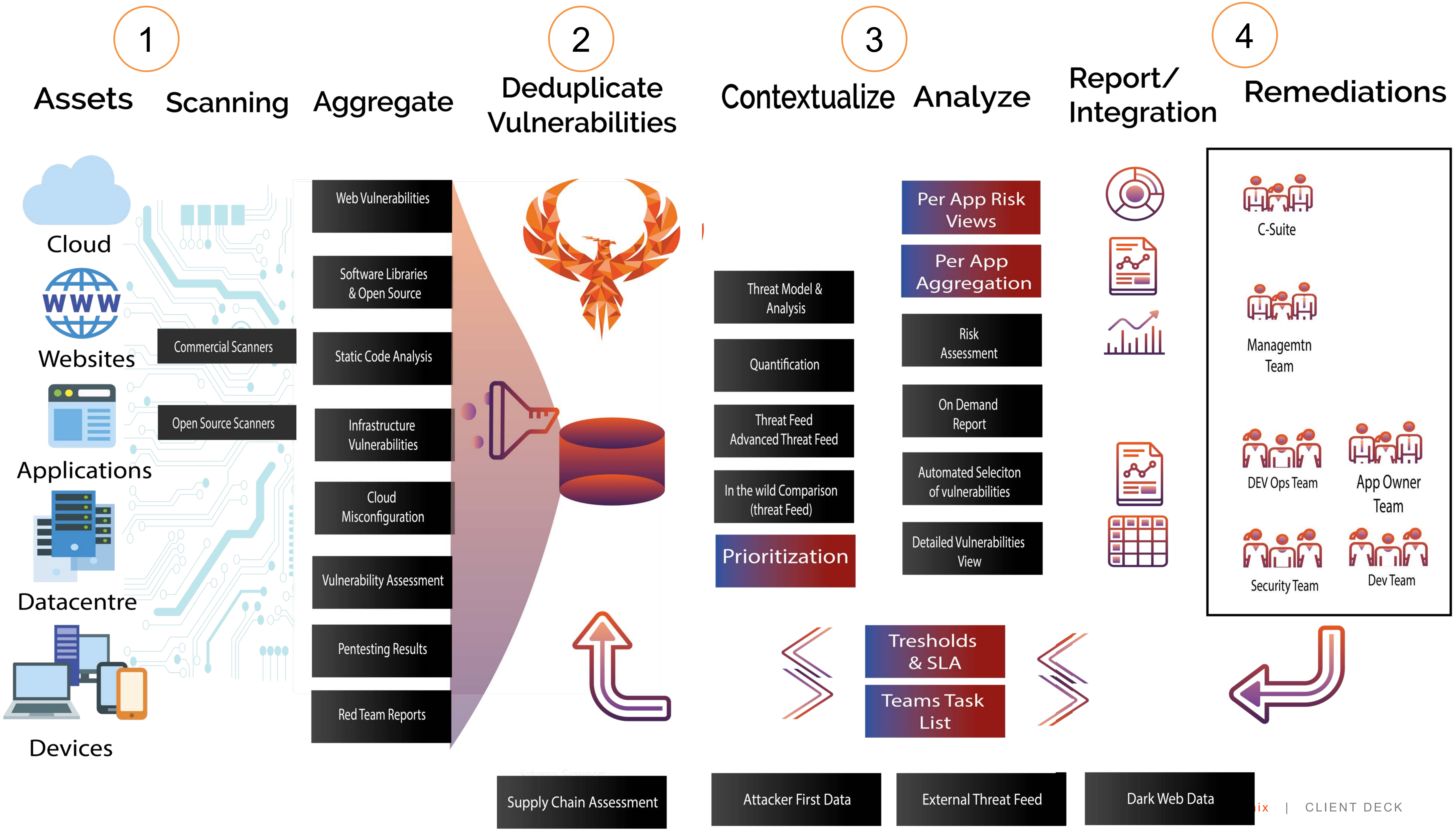


Critical	345	(40%)
High	288	(33%)
Medium	46	(5%)
Low	107	(12%)
Info	84	(10%)

Risk fixed: 18 out of 870 1% 100%

- Simple to use interfaces
- Centralize Vulnerabilities prioritized and risk scored
- End 2 End workflow with integration in development tools
- Prioritized vulnerabilities with business and external factors
- Industry data & Insight
- Threat feed
- Insights in Dark Web, Data breaches and 3rd party security posture

Flow



1

Assets

Scanning

Aggregate

2

Deduplicate Vulnerabilities

3

Contextualize

Analyze

Report/ Integration

4

Remediations

Cloud

Websites

Applications

Datacentre

Devices

Commercial Scanners

Open Source Scanners

Web Vulnerabilities

Software Libraries & Open Source

Static Code Analysis

Infrastructure Vulnerabilities

Cloud Misconfiguration

Vulnerability Assessment

Pentesting Results

Red Team Reports

Threat Model & Analysis

Quantification

Threat Feed Advanced Threat Feed

In the wild Comparison (threat Feed)

Prioritization

Per App Risk Views

Per App Aggregation

Risk Assessment

On Demand Report

Automated Seleciton of vulnerabilities

Detailed Vulnerabilities View

C-Suite

Managemtn Team

DEV Ops Team

App Owner Team

Security Team

Dev Team

Tresholds & SLA

Teams Task List

Supply Chain Assessment

Attacker First Data

External Threat Feed

Dark Web Data

How does it Works

1 Vulnerability Scan

2 Vulnerability Deduplication & Enrichment (INT/EXT)

3 Target Set, Reporting & Tasks Selection

Cloud
Websites
Applications
Datacentre
Devices
Commercial Scanners
AppSec Scanner
Rescan
CMDB/ BIA
Business Intelligence
Customer Treat Intel
Public Treat Intel
Phoenix Treat Intel
Attacker Treat Intel
Business SLA
Business Risk Appetite
AppSec Business intelligence
Threat Model & Analysis
Quantification
AppSec Business Threat Intelligence
Threat Feed Advanced Threat Feed
In the wild Comparison (threat Feed)
AppSec Risk Engine
Application Risk
External Surface
Application Attackability
Aggregated Risk
Component Risk
Vulnerabilities External Surface
Vulnerabilities Density
Vulnerabilities Risk
Vulnerabilities External Surface
Vulnerabilities Attackability
Cloud / Infrastructure
AppSec Prioritization Engine
Prioritization
Application Impact
Executive Target
Business Vulnerability SLA
External Industry Time to Fix SLA
Web Vulnerabilities to attack surface
AppSec Reporting
Teams Task List
Organization Risk Level
Vulnerability Systemic issues
Apps in/out Target
Organization Heatmap
Exec Reports
Apps Reports
Dev Tasks
Remediation Tracking

Find Vulnerabilities in Code, Libraries, Infrastructure, O/S, Cloud

Remove False Positives and duplicates

Enrich with Business intelligence (impact)

Compute Risk

Prioritize Vulnerabilities

THANK YOU FOR LISTENING

GET IN TOUCH

PHONE/ EMAIL

M: +44(0)7578 956956
E- f.c@appsecphoenix.com
E- sales@appsecphoenix.com

ADDRESS

Kemp House,
152 City Road
EC1V 2NX

www.appsecphoenix.com

Fix Vulnerability Today Before attacker exploit them tomorrow

OUR PLEDGE FOR RACIAL EQUALITY, DIVERSITY & INCLUSION

At AppSec Phoenix, our guiding principle is to change the status quo and be equal and better to inspire this and future generation to stand against racism, inequity and inequality

1. **Be Accountable and remove bias on wording, job specs**
2. **Encourage Feedback and correcting mistake**
3. **Speaking Up against racism and unjust**
4. **Diversify my network inside and outside AppSec Phoenix**
5. **Defend, Protec, Support and grow the next generation**

https://www.appsecphoenix.com/principles/

APPSEC PHOENIX

RESPECT IN SECURITY

RESPECT IN SECURITY PLEDGE

At AppSec Phoenix, we stand firm against racial and bullying hence we’ve committed and signed Respect in Security Pledge

1. **Eliminate Harassment, to include all employees, partners, customers, and interactions.**
2. **NOT Tolerate any form of harassment no matter what**
3. **Staff Members are will operate in a safe organisational or social environments.**
4. **Empower employees, and all the collaborators to come forward with reports**
5. **We will protect the anonymity.**
6. **We will regularly educate employees and contractors on what is harassment**
7. **We will regularly discuss reporting protocol with our employees.**

https://www.appsecphoenix.com/respectincyberpledge/