#RSAC

RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **CSCS-T09**

Continuous Security - Integrating Pipeline Security

Vandana Verma Sehgal

Security Relations Leader
Snyk
@InfosecVandana

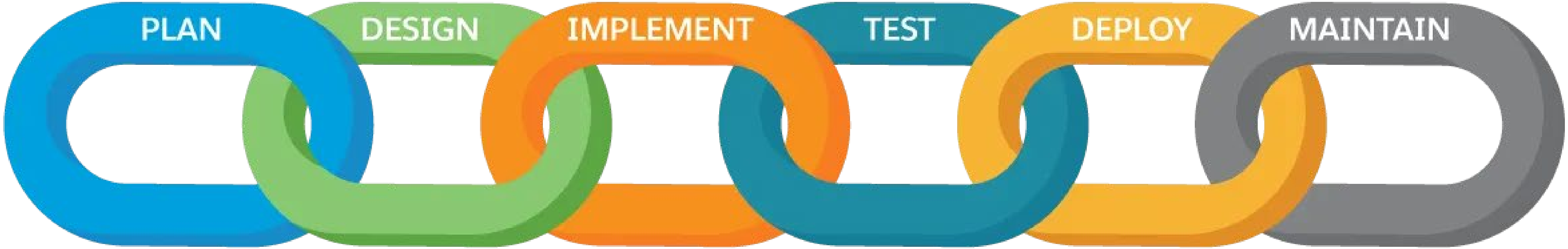
Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

WHO AM I

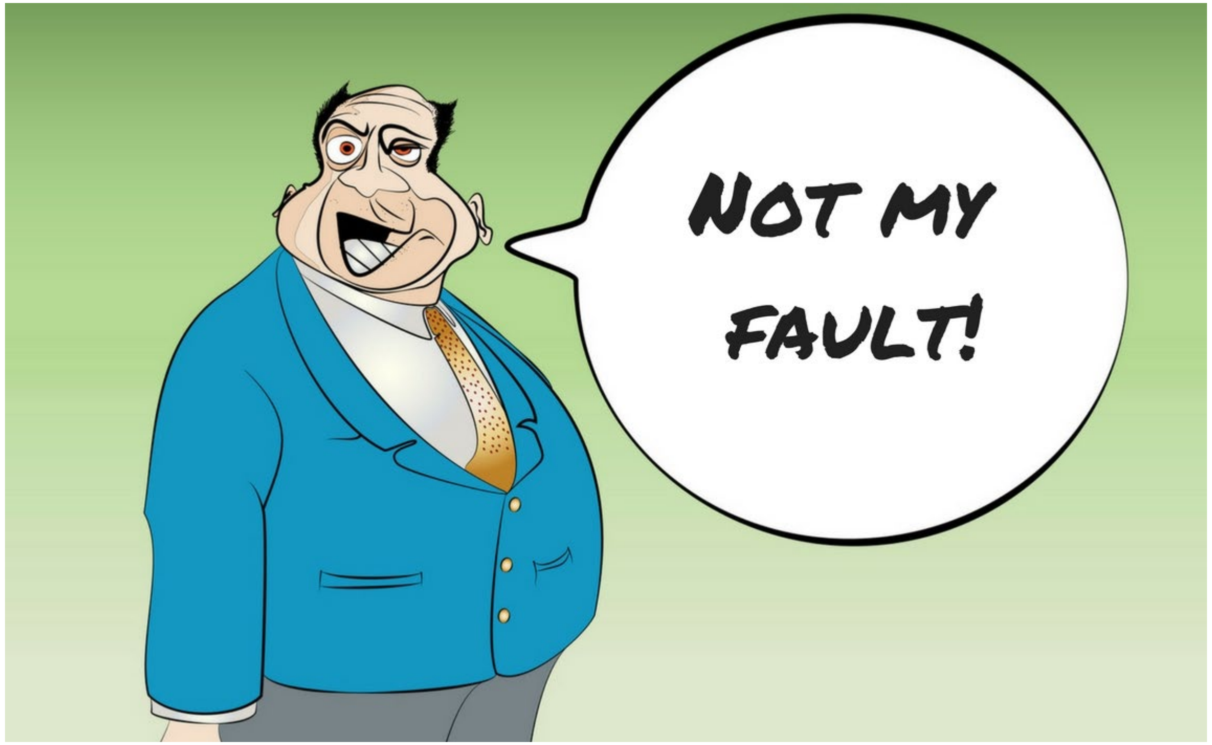
- Security Relations Leader - Snyk
- OWASP Global Board of Directors
- Speaker/Trainer at Defcon(AppSec Village), Asst. Trainer at Black Hat, OWASP AppSec Conferences and others
- Member of Review Board at Grace Hopper, BSides Delhi, Global AppSec, etc.


PLAN
DESIGN
IMPLEMENT
TEST
DEPLOY
MAINTAIN

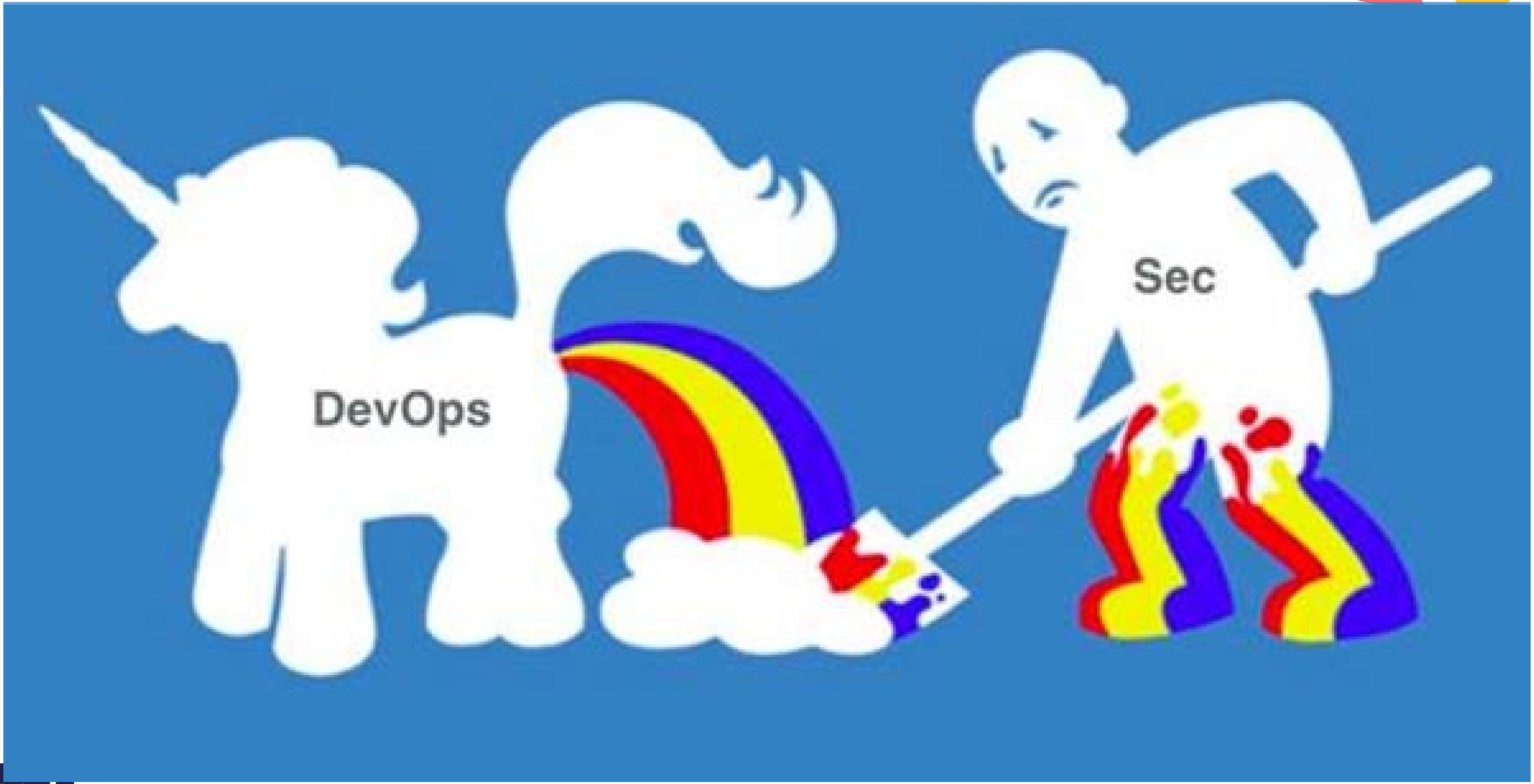
Blame Game

Security

Dev

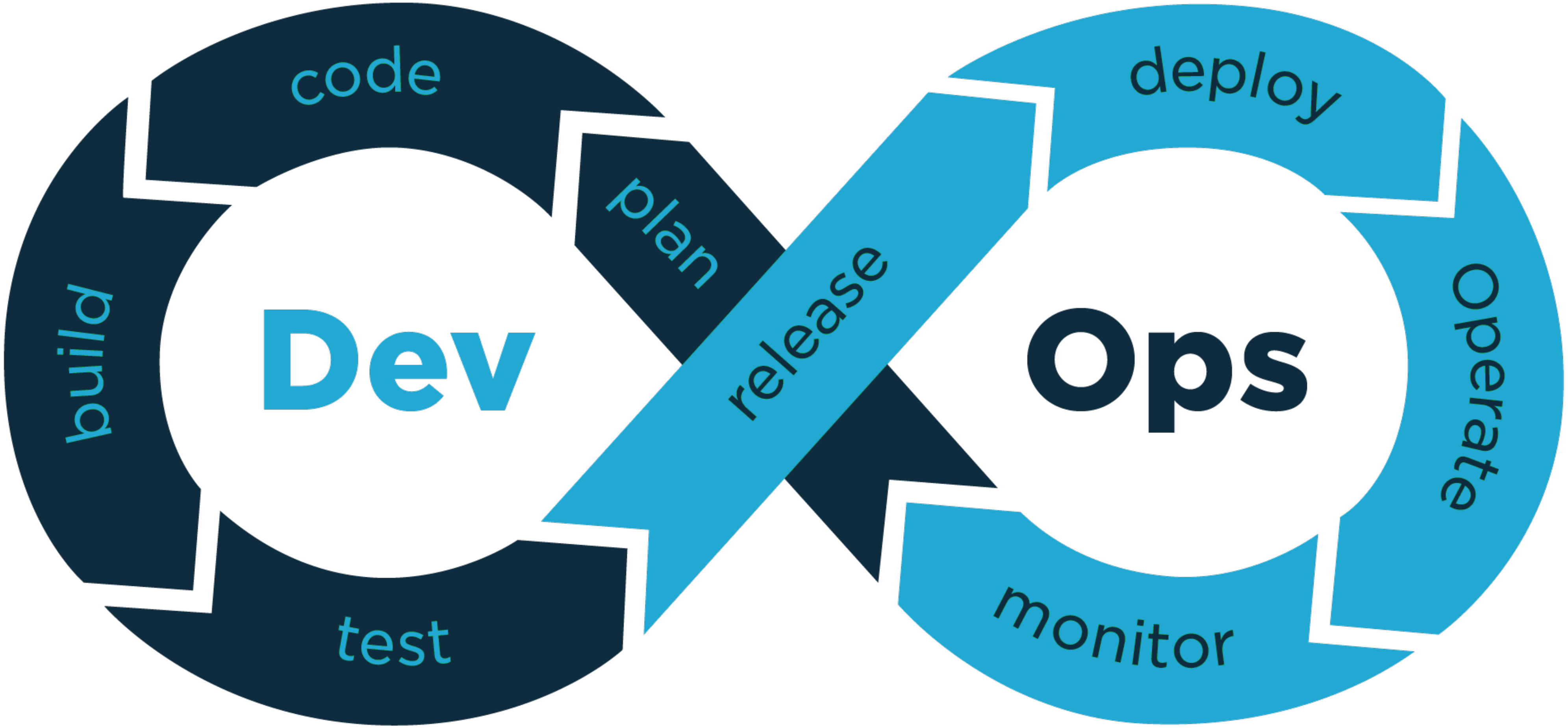


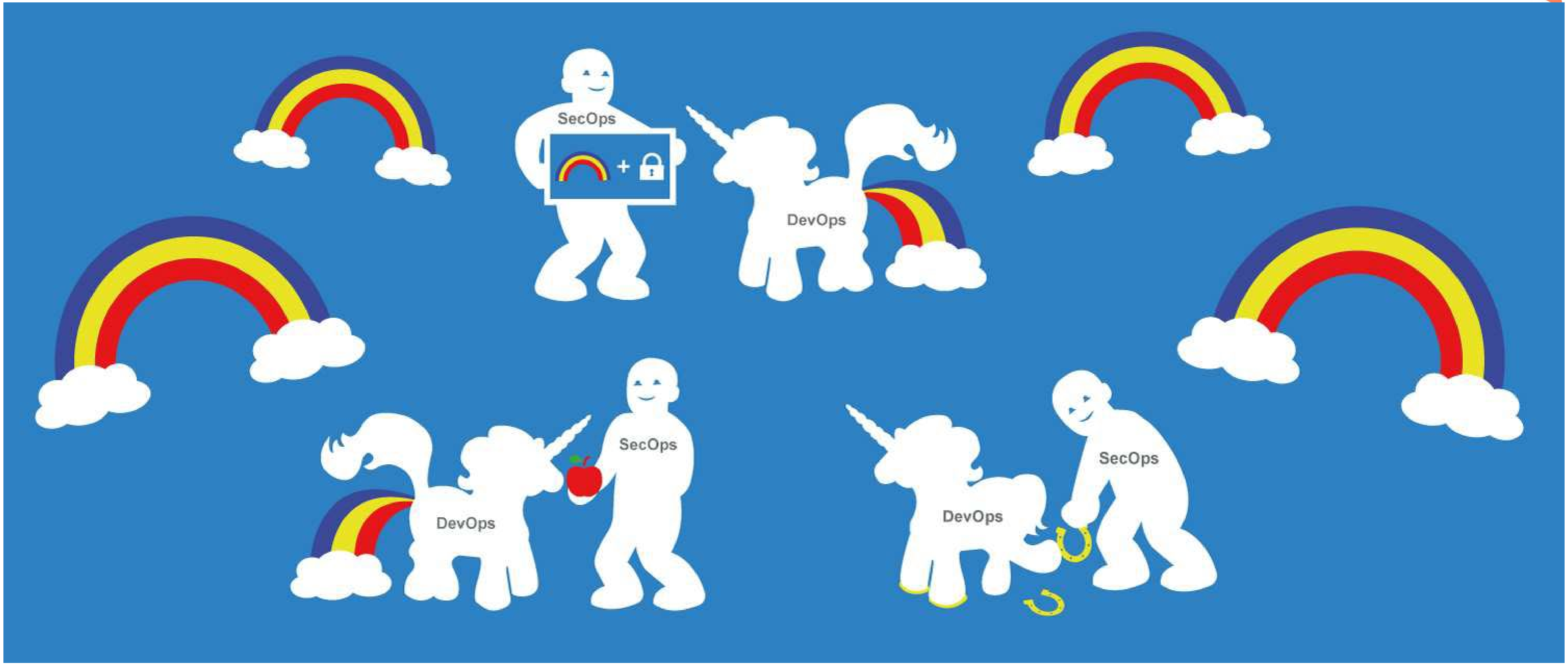
Ops



Slide Credit: Pete Cheslock

DevOps


code
plan
build
Dev
test
release
deploy
Ops
Operate
monitor



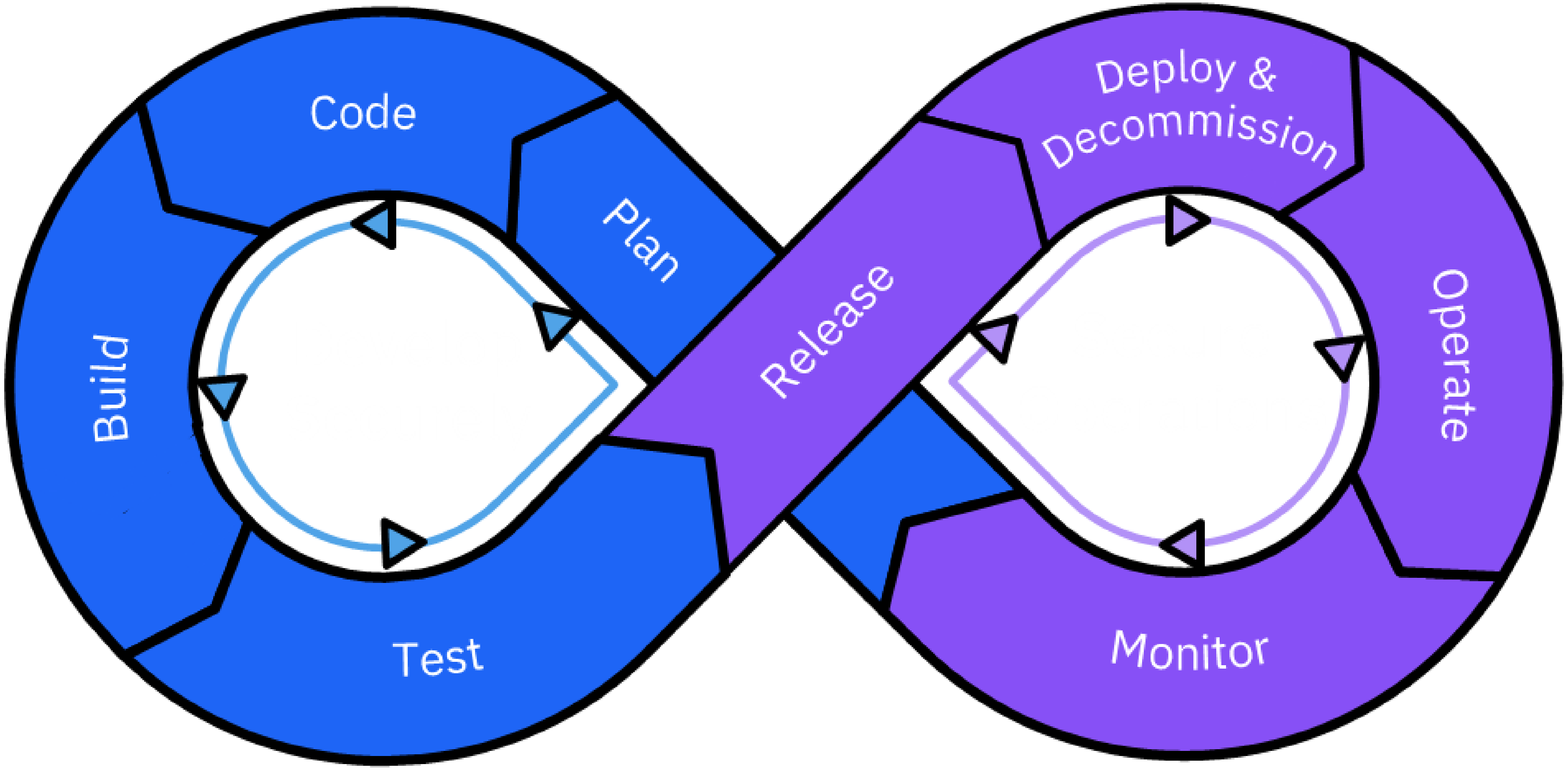
Slide Credit: DevSecCon

What is DevSecOps?

Integrating security practices within the DevOps process.

DevSecOps fosters a blameless culture and focused on secure delivery of software.

Integrating Security with DevOps to create DevSecOps



DevSecOps core principles

“ DevSecOps is an **approach**, a mindset,
a combination of **culture**, **process** and **technology** ”

“ You don’t **BUY** DevSecOps, you **DO** DevSecOps ! ”

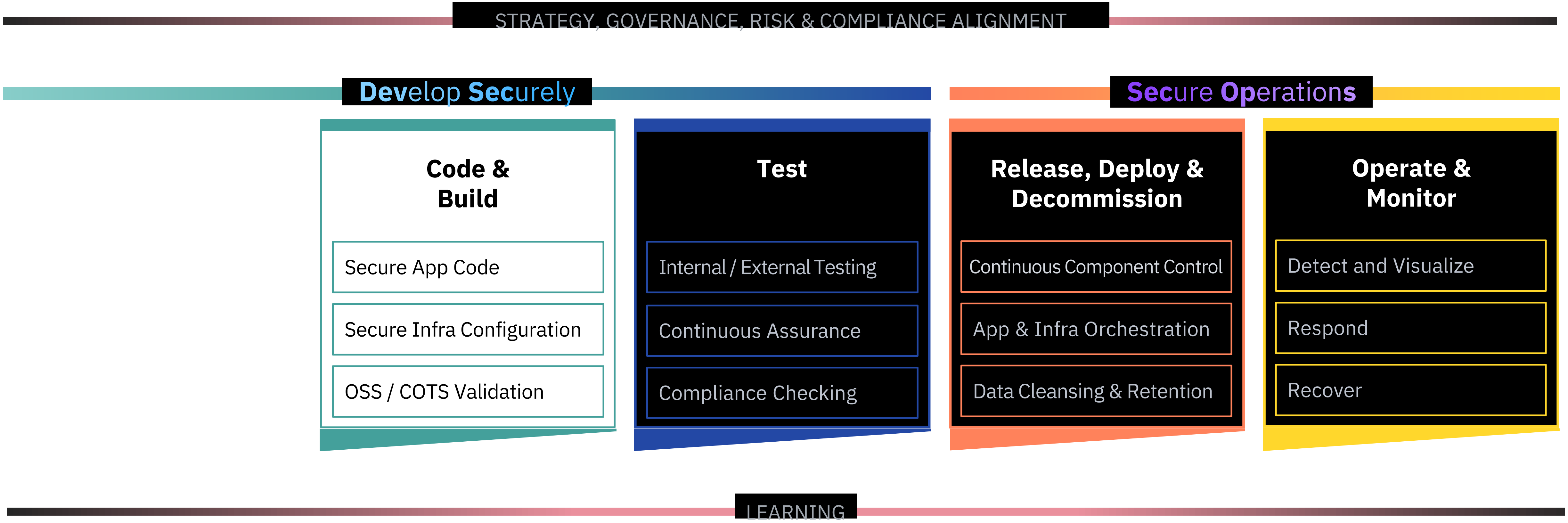
- **C**ulture
  - Agile, Lean and Continuous Feedback mindset applied throughout the Software Delivery Factory

- **A**utomation
  - Automate everything, everywhere for speed and reliability, using modern automation tools

- **M**easureme nt
  - Monitor everything, everywhere for Continuous Feedbacks, Improvement and Quality Management

- **S**haring
  - Share, coach, promote closer collaboration and process alignment between lines of business, development, and IT operations

People & Culture



STRATEGY, GOVERNANCE, RISK & COMPLIANCE ALIGNMENT

Develop Securely

Secure Operations

Code & Build

- Secure App Code
- Secure Infra Configuration
- OSS / COTS Validation

Test

- Internal / External Testing
- Continuous Assurance
- Compliance Checking

Release, Deploy & Decommission

- Continuous Component Control
- App & Infra Orchestration
- Data Cleansing & Retention

Operate & Monitor

- Detect and Visualize
- Respond
- Recover

LEARNING

Why does this matter?

Security practices must keep up with the agile pace of the cloud era.

Traditional Workload Provisioning	Cloud Workload Provisioning
Longer planning cycles More infrequent deployment schedules	**More agile approach** Deployments more iteratively as needed
Large, custom deployments	**Smaller, more standardized deployments**
Mostly manual deployment	**Highly automated and self-service for speed**
Siloed goals and objectives Separate development & operations teams	**Development + Operations to "DevOps"** Align objectives & remove tension between the groups

People & Culture

A successful program starts with the people & culture.

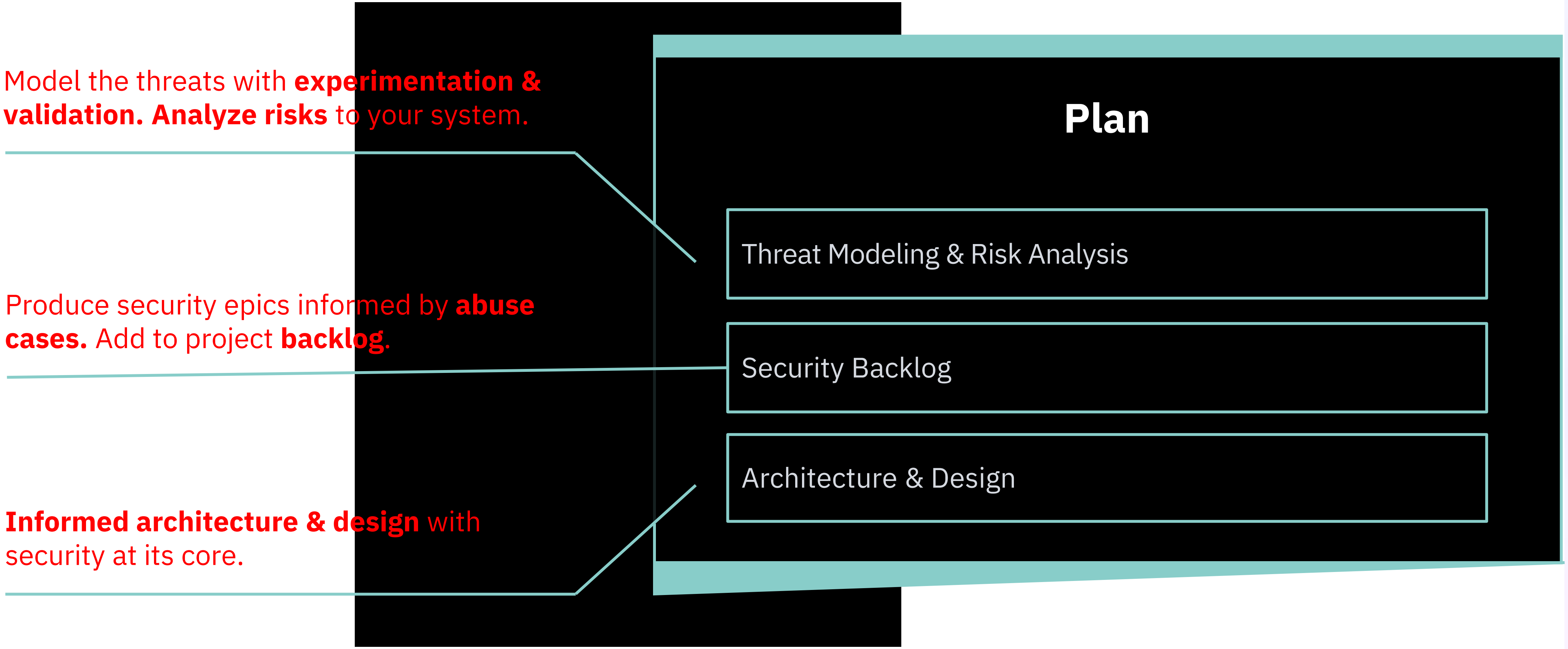
Training & Awareness

Explain & embrace new ways of working

Equip teams & individuals with the right level of ownership & tools

Develop Securely: Plan

A security-first approach



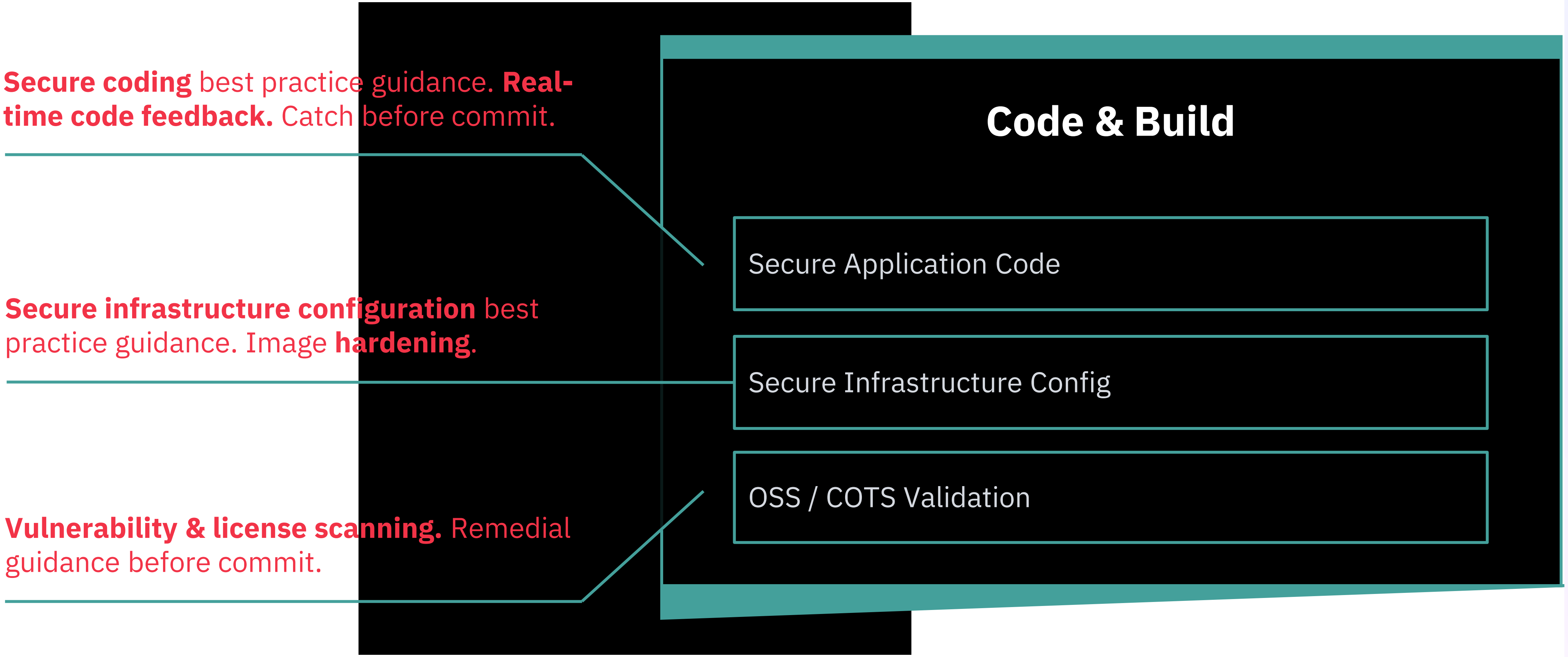
Model the threats with **experimentation & validation. Analyze risks** to your system.

Produce security epics informed by **abuse cases.** Add to project **backlog**.

Informed architecture & design with security at its core.

Develop Securely: Code & Build

Security & Development combined



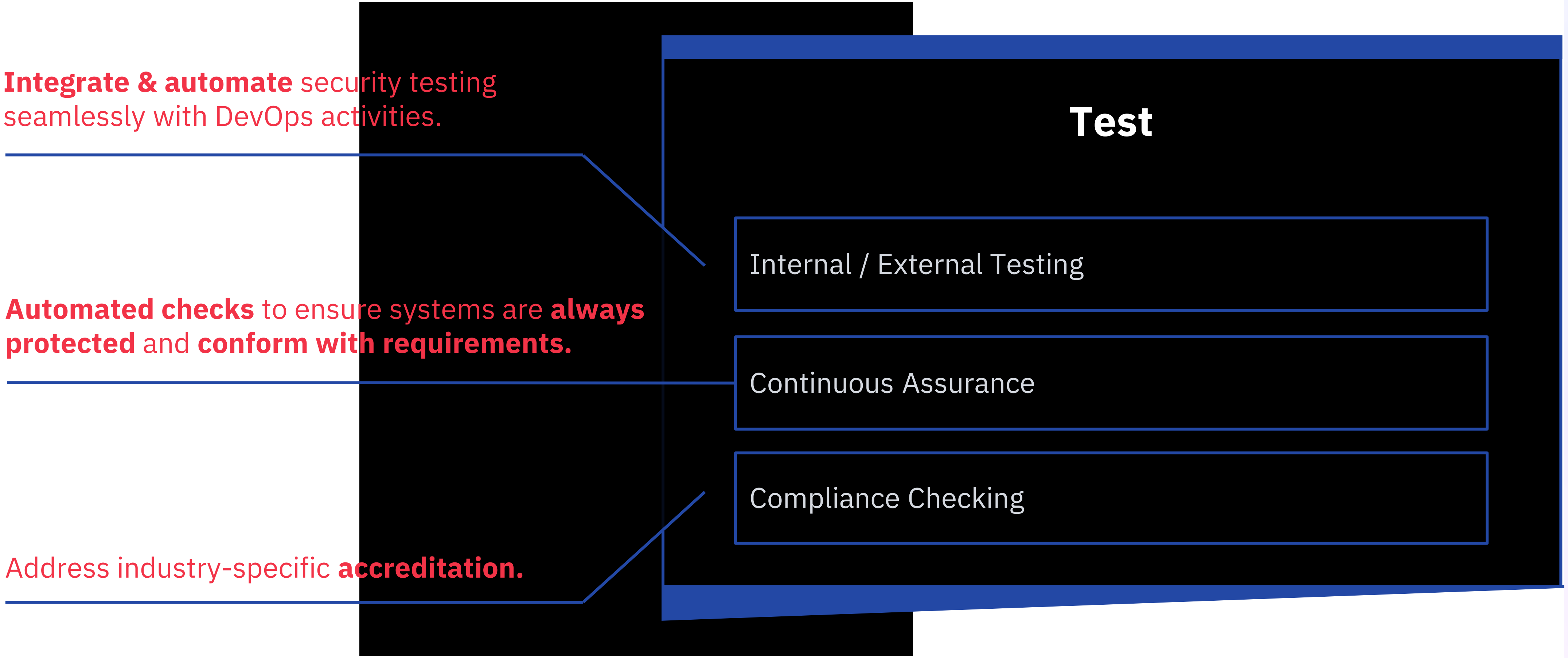
Secure coding best practice guidance. **Real-time code feedback.** Catch before commit.

Secure infrastructure configuration best practice guidance. Image **hardening**.

Vulnerability & license scanning. Remedial guidance before commit.

Develop Securely: Test

Security & Development combined



Integrate & automate security testing seamlessly with DevOps activities.

Automated checks to ensure systems are **always protected** and **conform with requirements.**

Address industry-specific **accreditation.**

Test

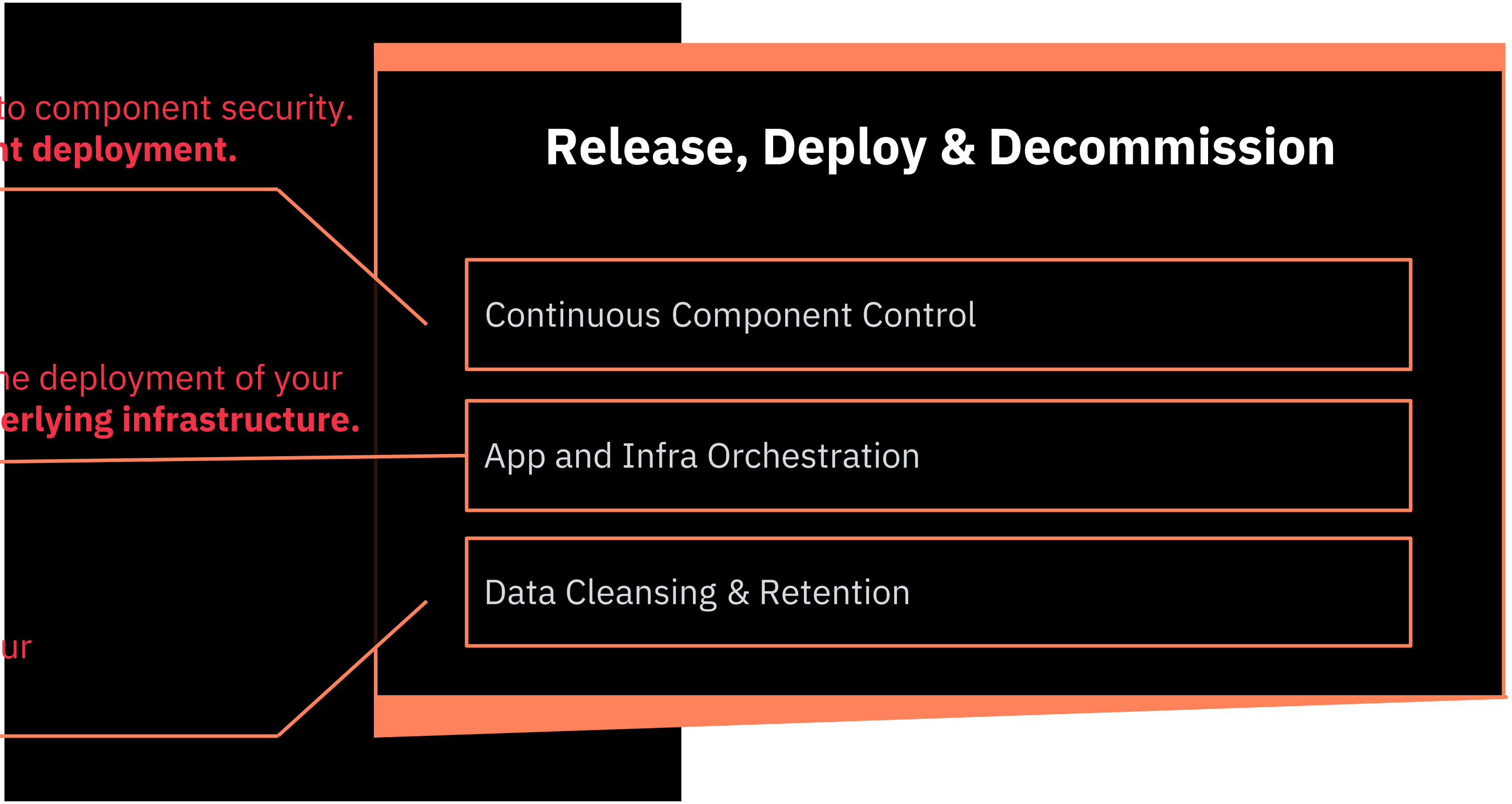
Internal / External Testing

Continuous Assurance

Compliance Checking

Secure Operations: Release, Deploy & Decom

Controlled creation & destruction



Release, Deploy & Decommission

- Continuous Component Control
- App and Infra Orchestration
- Data Cleansing & Retention

Monitor and act on changes to component security. **Block vulnerable component deployment.**

Orchestrate and automate the deployment of your **secure application** and **underlying infrastructure.**

Build **data cleansing** into your decommissioning activities.

Learning

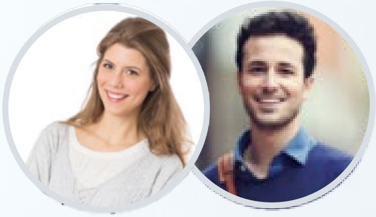
Continuous improvement and feedback.

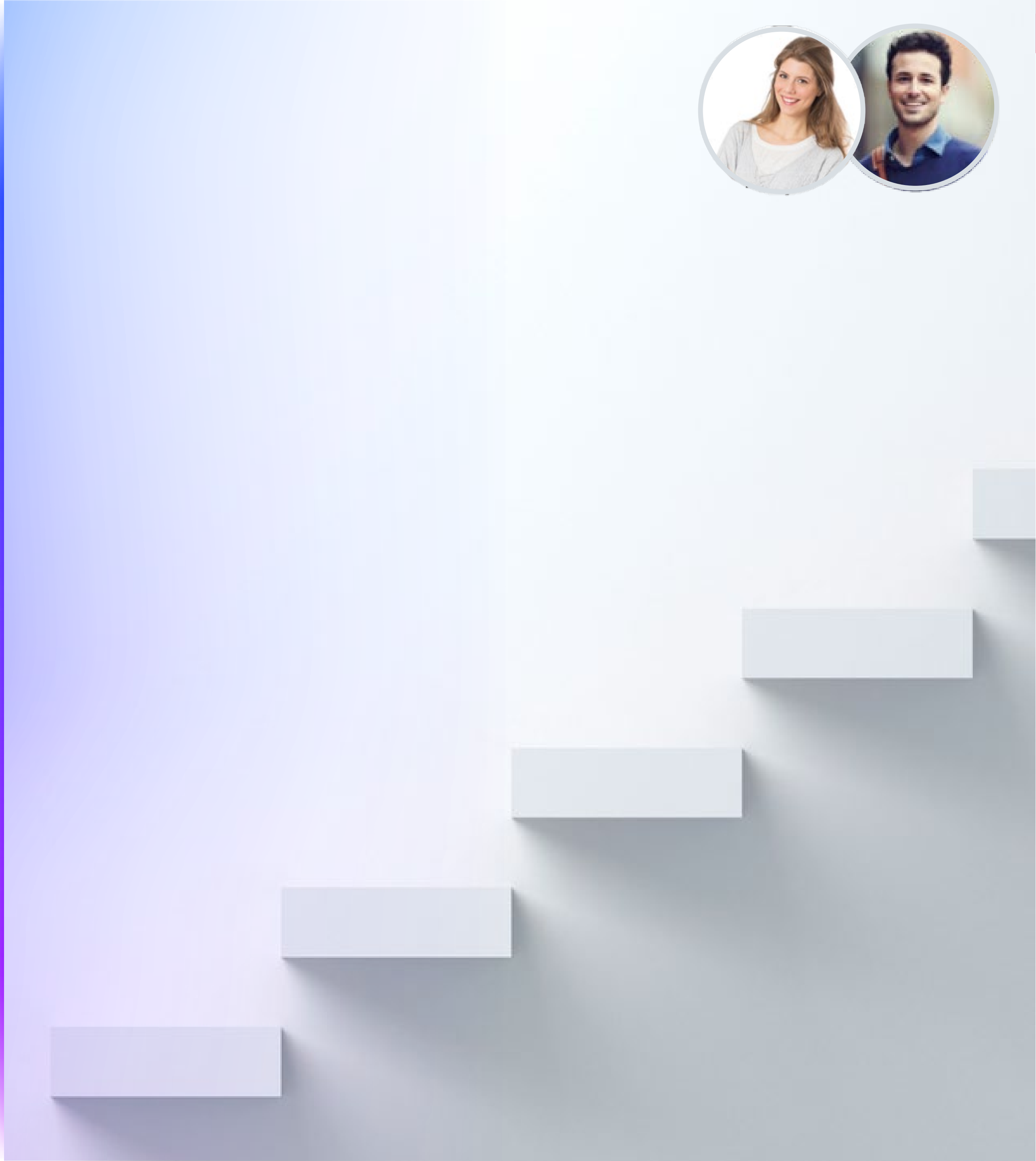
Lessons learned

Coding & tooling best practices level-set

Ongoing collaboration

Blameless post-mortems





So, why DevSecOps?

Reduce Risk & Cost
Fix early & bake in DR to reduce cost & risk

Increase Quality
Continuous monitoring & scanning

Improve Team Synergy
Increased collaboration & productivity

Enhance Visibility
Threat Management integration

Meet Compliance
Address critical compliance requirements

Accelerate Development
Security automation integrated into CI/CD pipeline

Secure, Rapid Innovation
Satisfy DevOps and CISO requirements

Things to manage

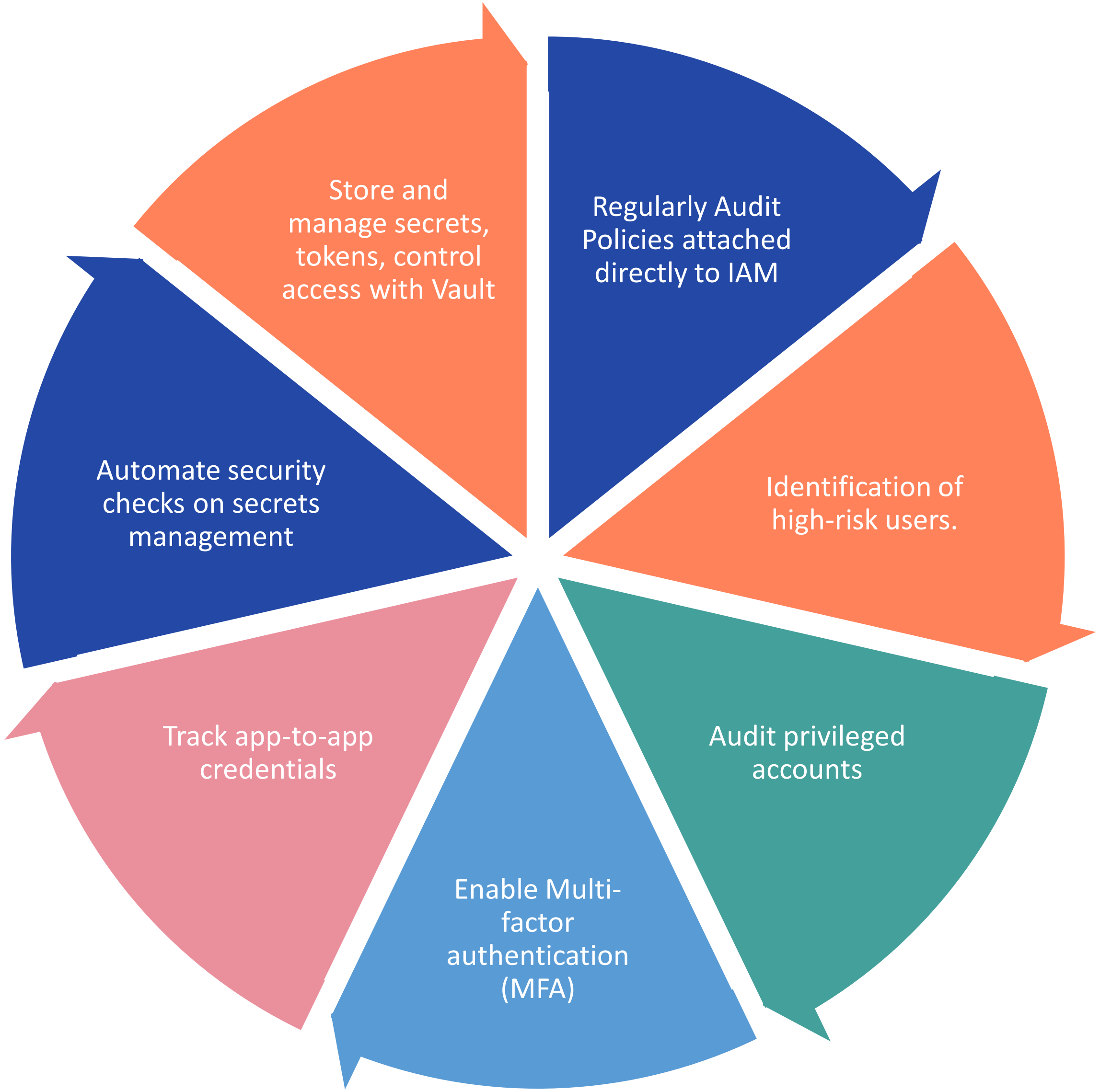
Asset Management

- Asset Tagging is as important as any other task in the organisation - tagging to right resources to the right owners.
- Maintain the CMDB (Configuration Management Database)
- Define asset onboarding or offboarding process
- Periodic review and update CMDB

Risk Management

- Understand the threat landscape for the organisation and applications
- ✓ Perform threat modelling
- Automate the threat modelling as a code (TaaC)
- Document the threat Model Process
- Risk Acceptance from the relevant stake holders.

Identity and Access management (IAM)



Regularly Audit Policies attached directly to IAM

Identification of high-risk users.

Audit privileged accounts

Enable Multi-factor authentication (MFA)

Track app-to-app credentials

Automate security checks on secrets management

Store and manage secrets, tokens, control access with Vault

Embrace the automation

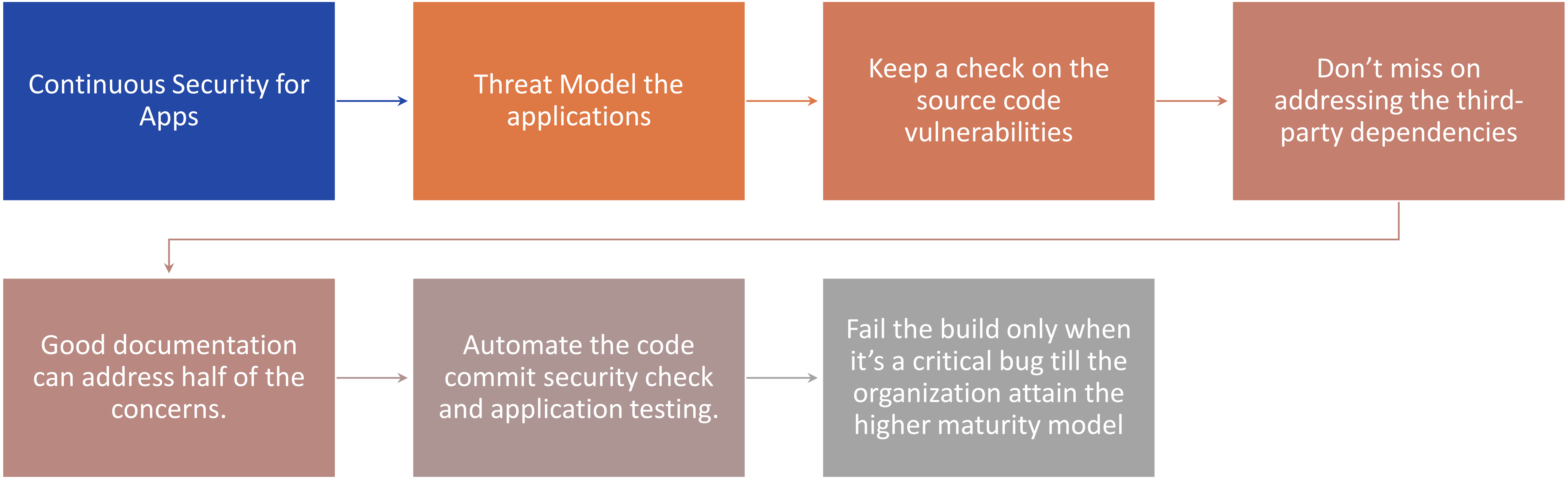
Pic souce:-https://blogs.iadb.org/caribbean-dev-trends/wp-content/uploads/sites/34/2019/06/CCB-Automation-blog.jpg

Vulnerability Management

- Perform regular vulnerability assessments
- Defining the custom priorities of identified vulnerabilities based on the environment
- Create a patching plan
- Follow the change management process
- Test the patches in the test or dev environment
- Apply relevant patches to avoid the breaches
- Perform rescan to ensure the vulnerability fix

snyk

Web Applications



Continuous Security for Apps

Threat Model the applications

Keep a check on the source code vulnerabilities

Don’t miss on addressing the third-party dependencies

Good documentation can address half of the concerns.

Automate the code commit security check and application testing.

Fail the build only when it’s a critical bug till the organization attain the higher maturity model

Empower Dev /Ops to deliver better and faster and secure, instead of blocking.

Governance, Risk and Compliance

- Implementation of configuration changes and policy rules
- Automate Compliance to run as a code (CaaC)
- Versioning is important to maintain code
- Setting up the process on when to fail the build in the pipeline.
- Create feedback loops to understand the Risks

Monitoring and Logging

1. On-boarding critical log sources (applications, servers, network devices, etc.)

2. Enable required logs (e.g application logs, platform logs, security logs etc.)

3. Building use cases to capture critical activities

4. Continuous monitoring of the production environment for exploitation of known/unknown vulnerabilities.

5. Prepare the response plan to handle the incidents.

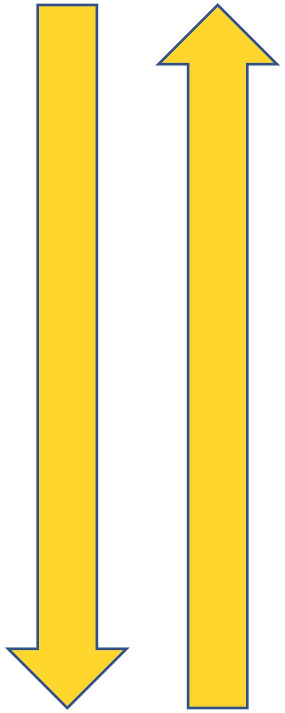
Emergency Response

- Documented plan for handling the critical incidents
- Agreed RACI (Responsible, Accountable, Consulted and Informed) Matrix
- Identify the right stakeholders
- Documented escalation matrix
- High severity incident creation with the bridge (call) details
- Knowing the Disaster Recovery (DR) plan
- High Availability (HA) setup for critical assets

Cultural Shift

Top Down Approach

- Let developers lead the way
- Organizational transparency
- Breaking Down Barriers and Silos



- Teams collaboration and inclusive culture
- Build Champions and collaborate them
- Speak in executives speak!

Bottom Up Approach

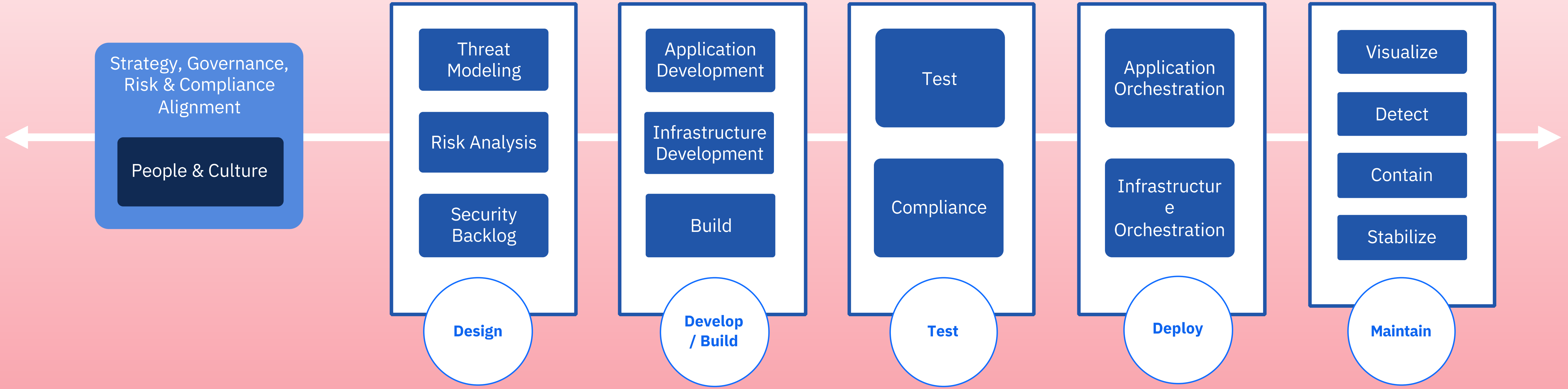
Tools of Trade

Threat Modelling Tools	THREAT PLAYBOOK ThreatSpec Microsoft Threat Modeling Tool
Pre-Commit Hooks	Talisman P git-secret truffleHog Git Hound
Software Composition Analysis	D DEPENDENCY-CHECK Requires.io Retire.js
Static Analysis Security Testing (SAST)	Bandit BRAKEMAN RIPS sonarqube Pmd DON'T SHOOT THE MESSENGER
IDE Plugins	devskim CAT.net ™
Secret Management	HashiCorp Vault Keywhiz Confidant

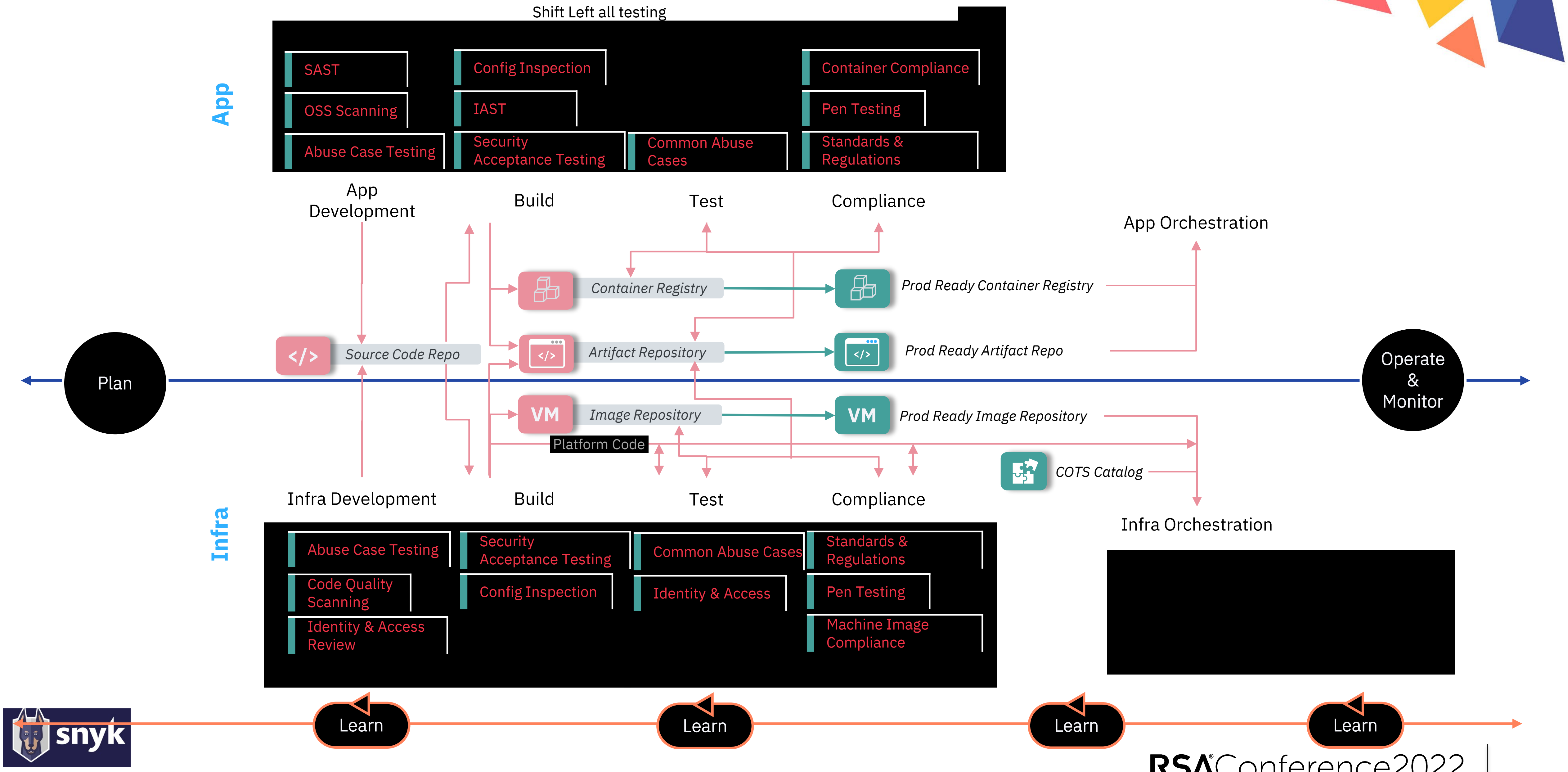
Ref: Anant Shrivastava

Vulnerability Management	ARCHERY a security tool JACK HAMMER DEFECTDOJO
Dynamic Analysis Security Testing (DAST)	arachni web application security scanner framework w3af Wapiti
Security in Infrastructure as Code	OpenVAS Open Vulnerability Assessment System anchore clair DOCKSCAN OpenSCAP
Compliance as Code	KitchenCI INSPEC DevSec Hardening Framework Docker Bench for Security
WAF	modsecurity Open Source Web Application Firewall NAXSI

DevSecOps Reference Architecture - Overview



Security DevSecOps Reference Architecture



Shift Left all testing

App

SAST

OSS Scanning

Abuse Case Testing

Config Inspection

IAST

Security Acceptance Testing

Common Abuse Cases

Container Compliance

Pen Testing

Standards & Regulations

App Development

Build

Test

Compliance

App Orchestration

Container Registry

Prod Ready Container Registry

Plan

Source Code Repo

Artifact Repository

Prod Ready Artifact Repo

Operate & Monitor

VM

Image Repository

VM

Prod Ready Image Repository

Platform Code

COTS Catalog

Infra Development

Build

Test

Compliance

Infra Orchestration

Infra

Abuse Case Testing

Code Quality Scanning

Identity & Access Review

Security Acceptance Testing

Config Inspection

Common Abuse Cases

Identity & Access

Standards & Regulations

Pen Testing

Machine Image Compliance

snyk

Learn

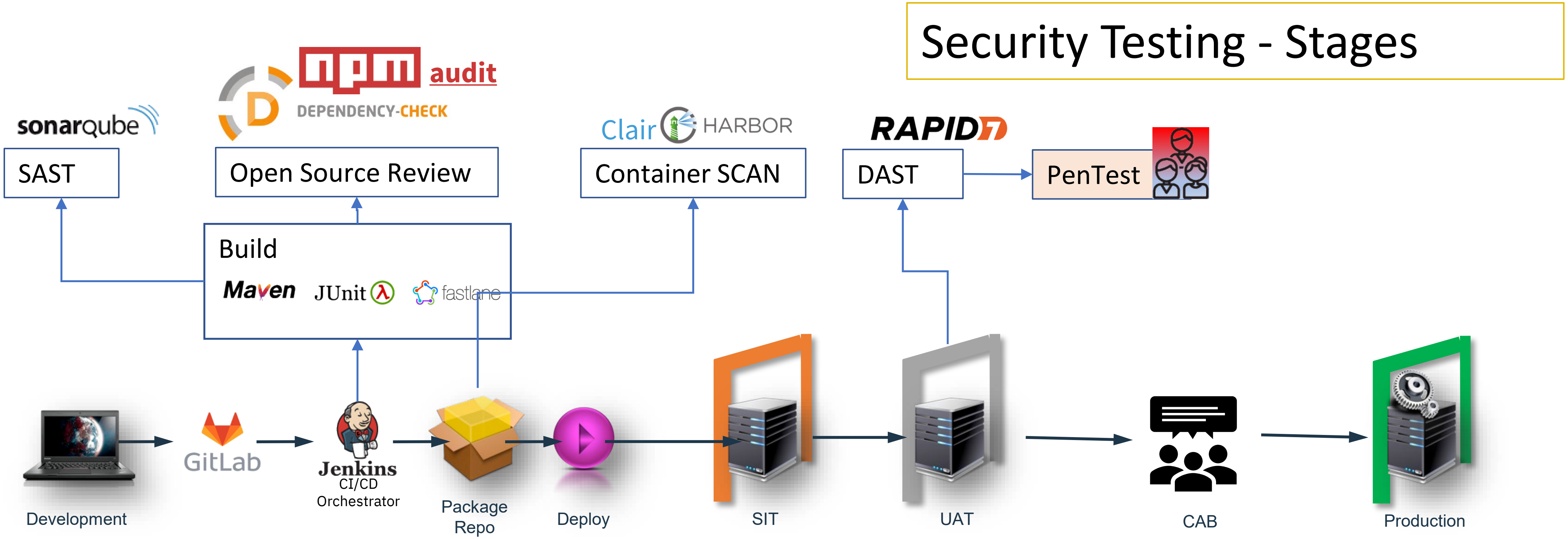
Learn

Learn

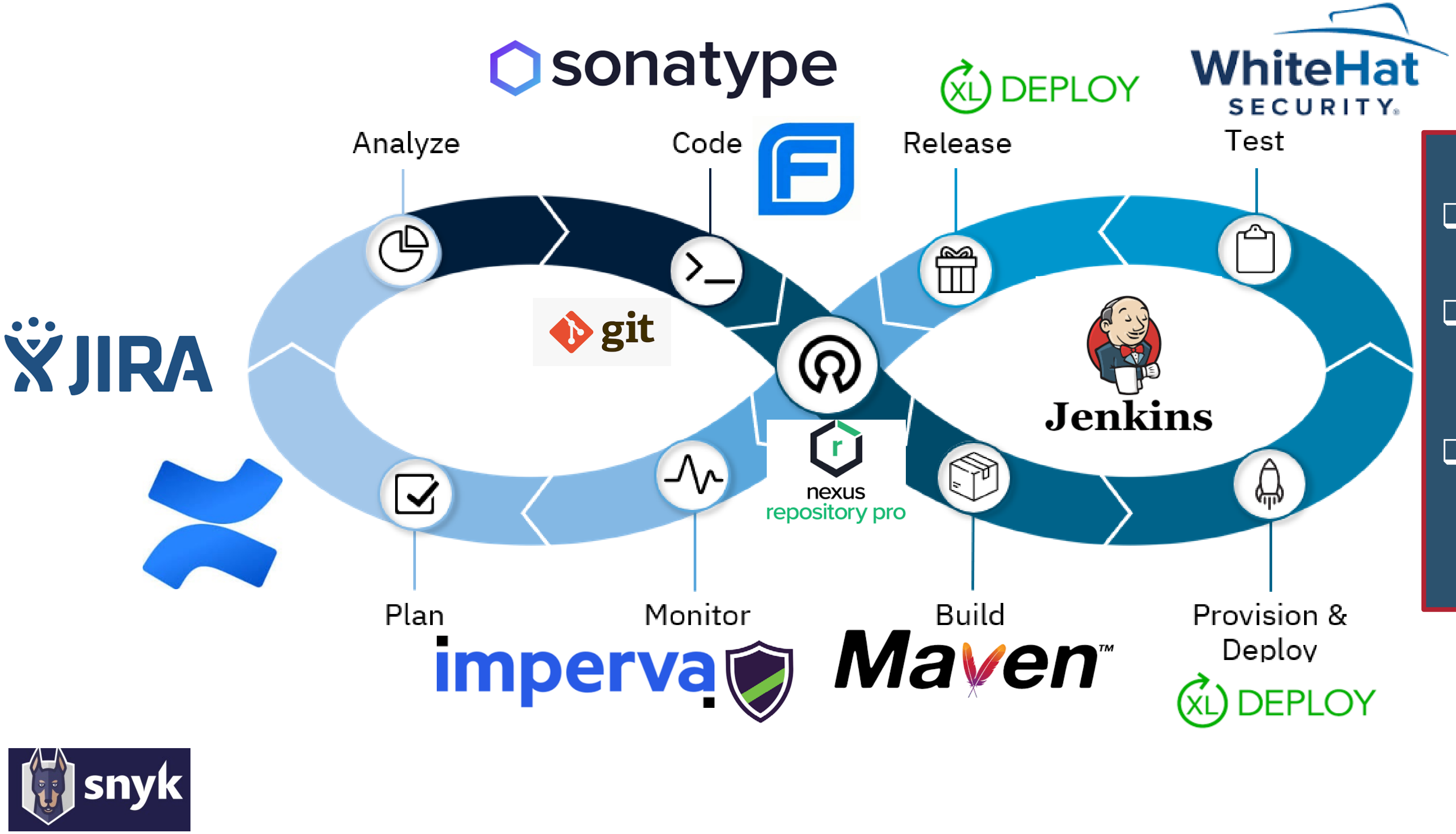
Learn

DevSecOps for a Large Bank in ASEAN

Project Profile: Bank is undergoing digital transformation journey and aims to use e-solutions platform to digitize branch process and customer journey.



A medium size Insurance company specializing in Retirement Plans and Employee Benefits



Highlights

- ❑ Vulnerability closing time is reduced to 2 sprints (from 4 sprints).
- ❑ Deployments to production did not require "Gone Fishing" page for 80% of the applications
- ❑ Successfully operationalized and transitioned ownership of SAST, DAST and remediation to LOB.

Reach Me!

- Twitter: @InfosecVandana
- LinkedIn: vandana-verma