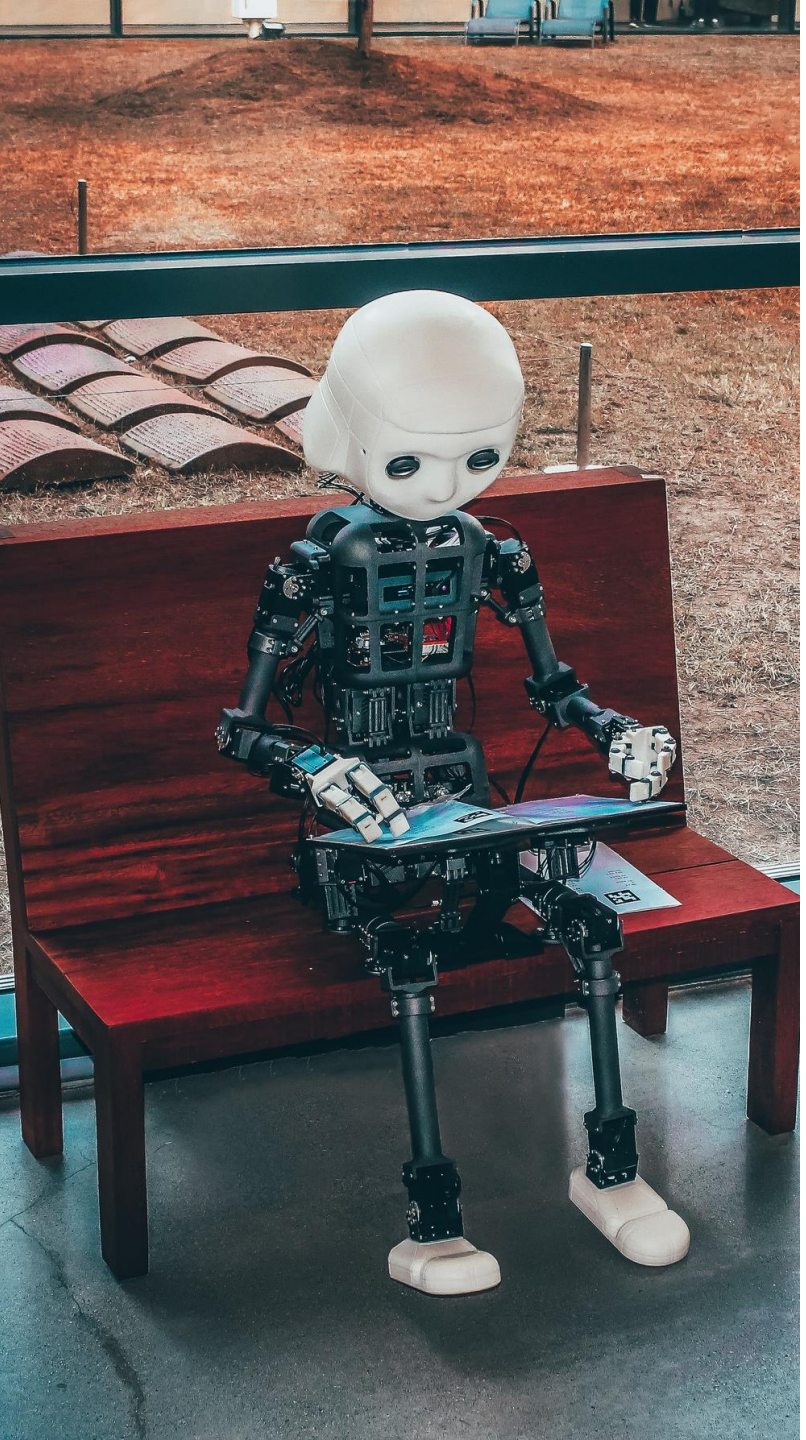


OWASP Projects and Tools to Secure Your SDLC

Raafey Khan

OWASP NZ | JULY 23

CyberCX

Me

Raafey Khan

Application Security | CyberCX

Why?

OWASP is great

Too many things

Guidance often talks about what not how

Everyone solves “DevSecOps” now?

Why?

OWASP is great

Too many things

Guidance often talks about what not how

Everyone solves “DevSecOps” now?

Why?

OWASP is great

Too many things

Guidance often talks about what not how

Everyone solves “DevSecOps” now?

Approach

1

Define the tools / processes needed

2

Find **OWASP projects** to meet each requirement

Find **OWASP endorsed projects** to meet each requirement

Find **open-source projects** to meet each requirement

3

(Later)

Test and build a program using these projects

Approach

1

Define the tools / processes needed

2

Find **OWASP projects** to meet each requirement

Find **OWASP endorsed projects** to meet each requirement

Find **open-source projects** to meet each requirement

3

(Later)

Test and build a program using these projects

Approach

1

Define the tools / processes needed

2

Find **OWASP projects** to meet each requirement

Find **OWASP endorsed projects** to meet each requirement

Find **open-source projects** to meet each requirement

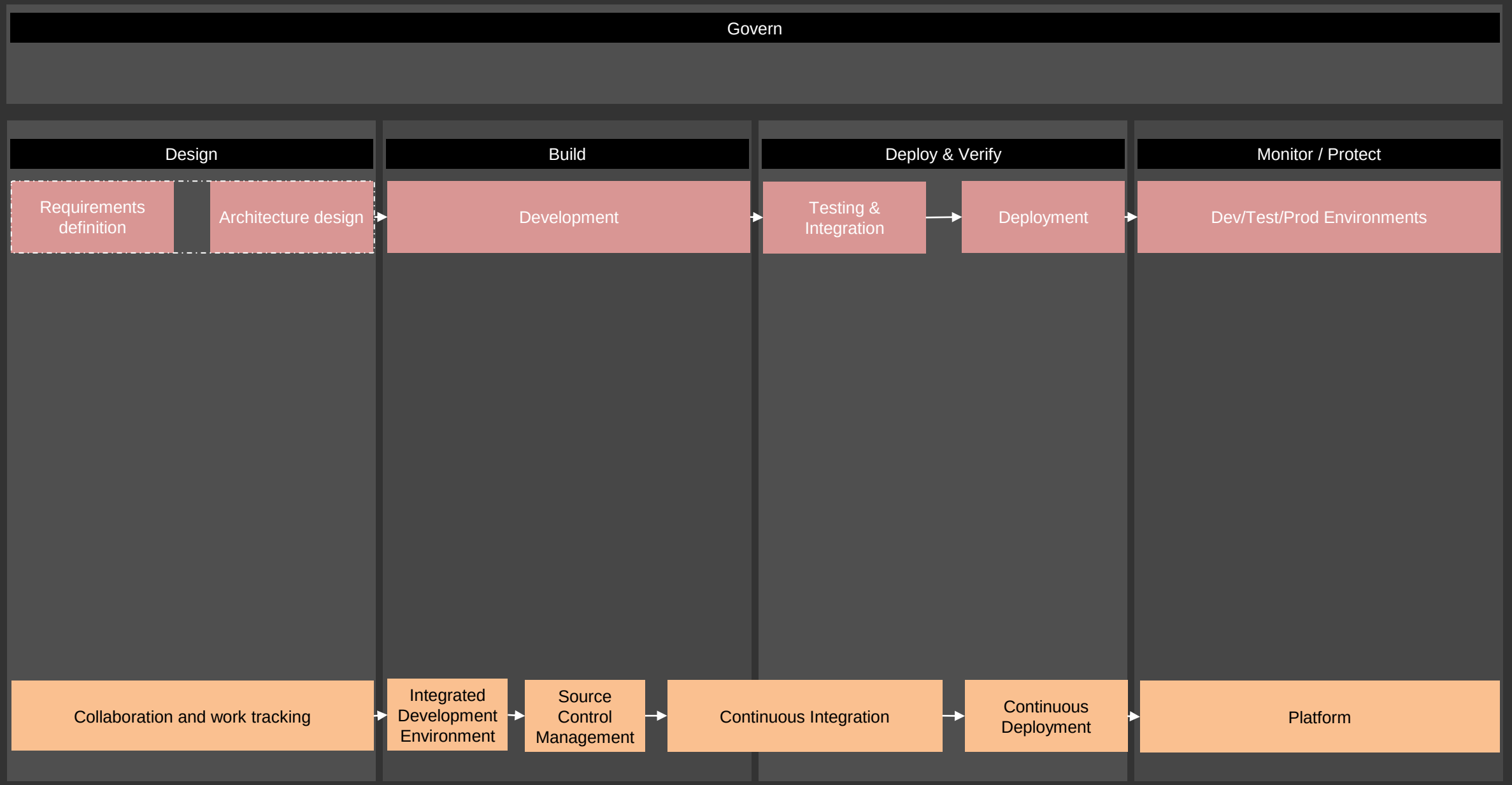
3

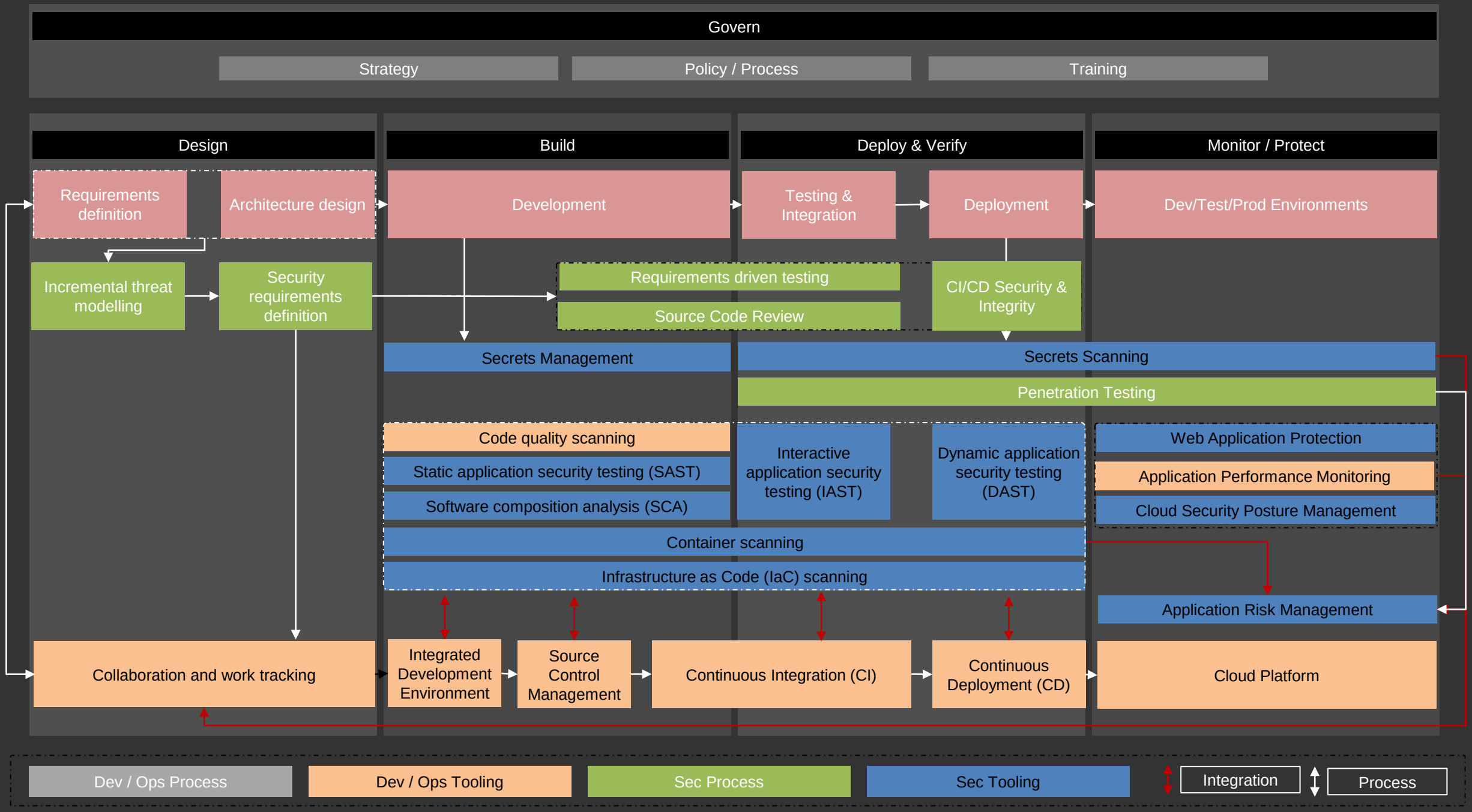
(Later)

Test and build a program using these projects

1. Define the Tools / Processes

The Secure SDLC


Govern
Design
Build
Deploy & Verify
Monitor / Protect
Requirements definition
Architecture design
Development
Testing & Integration
Deployment
Dev/Test/Prod Environments
Collaboration and work tracking
Integrated Development Environment
Source Control Management
Continuous Integration
Continuous Deployment
Platform


Govern
Strategy
Policy / Process
Training
Design
Build
Deploy & Verify
Monitor / Protect
Requirements definition
Architecture design
Development
Testing & Integration
Deployment
Dev/Test/Prod Environments
Incremental threat modelling
Security requirements definition
Requirements driven testing
Source Code Review
CI/CD Security & Integrity
Secrets Management
Secrets Scanning
Penetration Testing
Code quality scanning
Static application security testing (SAST)
Software composition analysis (SCA)
Interactive application security testing (IAST)
Dynamic application security testing (DAST)
Web Application Protection
Application Performance Monitoring
Cloud Security Posture Management
Container scanning
Infrastructure as Code (IaC) scanning
Application Risk Management
Collaboration and work tracking
Integrated Development Environment
Source Control Management
Continuous Integration (CI)
Continuous Deployment (CD)
Cloud Platform
Dev / Ops Process
Dev / Ops Tooling
Sec Process
Sec Tooling
Integration
Process

Govern

Govern

Strategy

Policy / Process

Training

Govern

Strategy

Policy / Process

Training

Security Champions playbook

Identify teams | Define the role | Nominate champions | Comm channels | Knowledge base | Maintain interest

SecureFlag

OWASP Secure Coding Practices Quick Reference Guide

OWASP Cheat Sheet Series

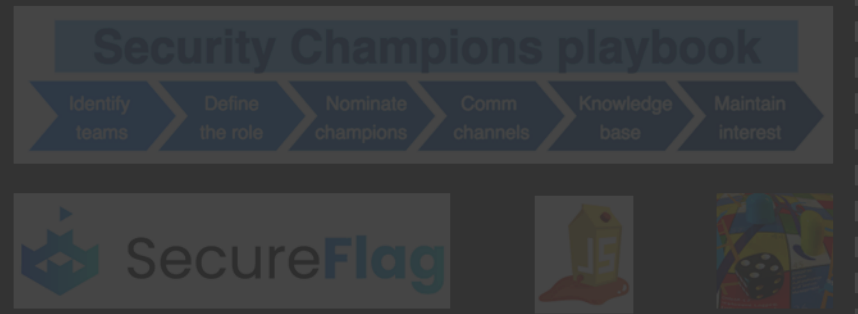
Govern

Strategy

Policy / Process

Training

OWASP SAMM



OWASP Secure Coding Practices
Quick Reference Guide

OWASP Cheat Sheet Series

*OWASP Partner

Govern

Strategy | Policy / Process | Training

OWASP SAMM

Security Champions playbook

Identify teams | Define the role | Nominate champions | Comm channels | Knowledge base | Maintain interest

SecureFlag*

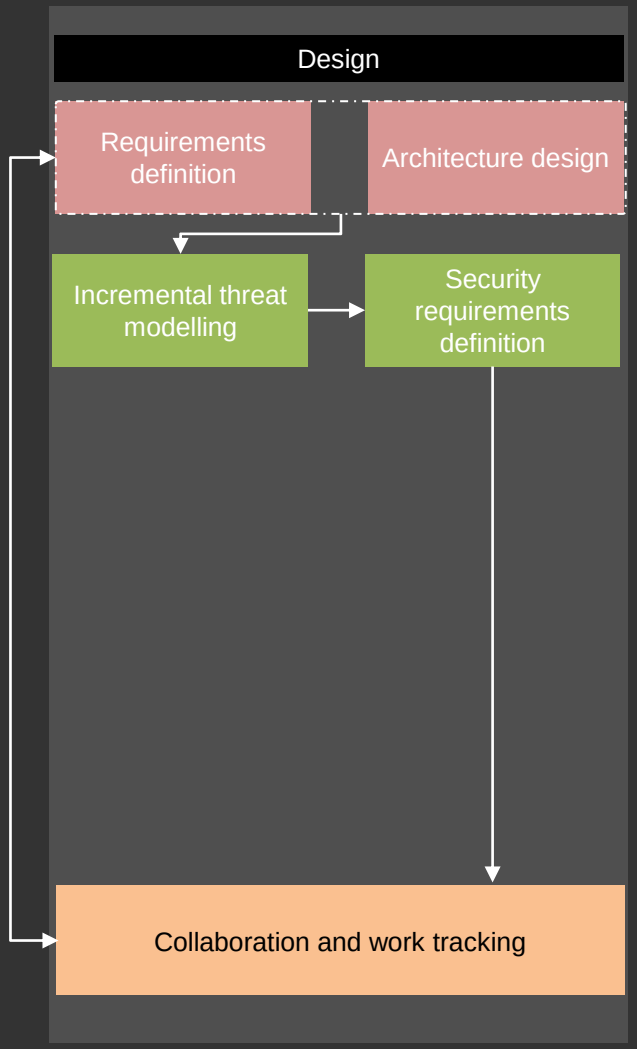
Juice Shop

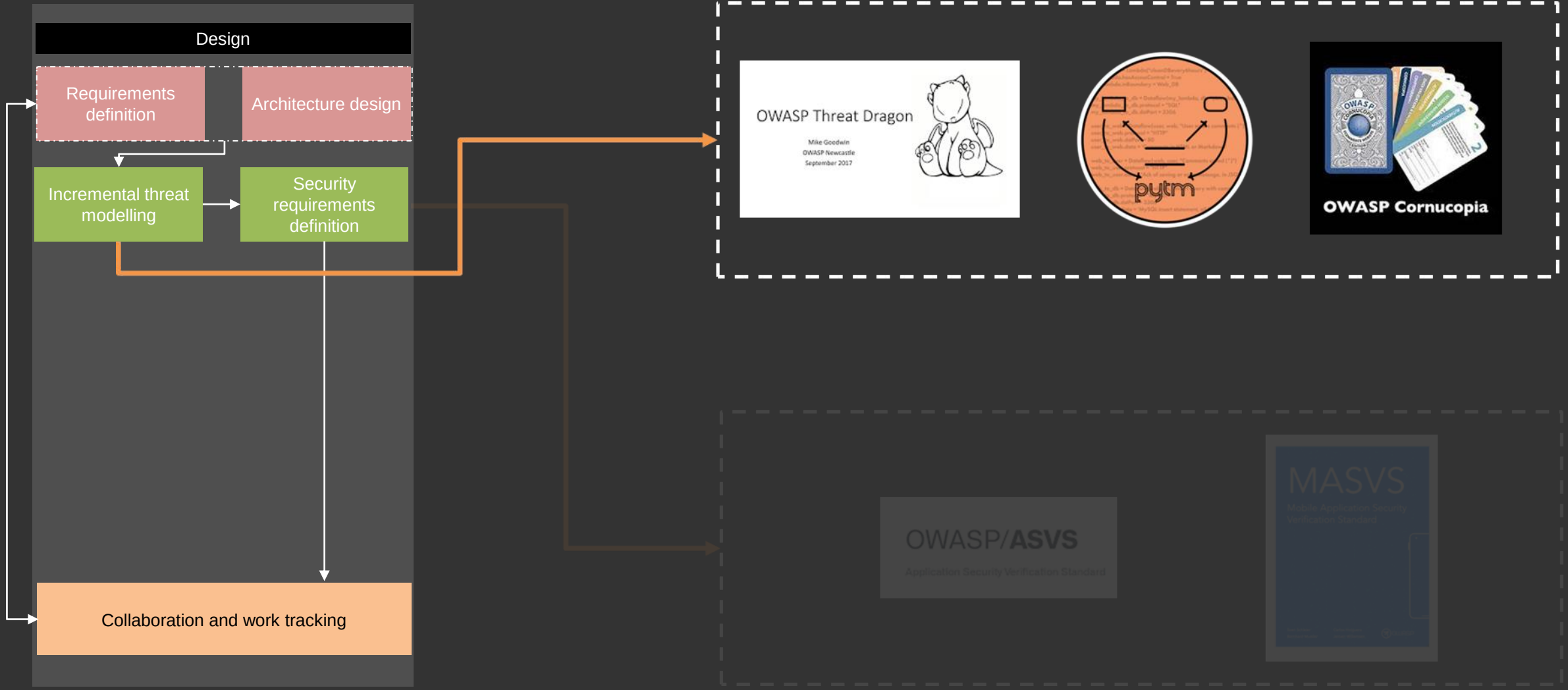
Cornucopia

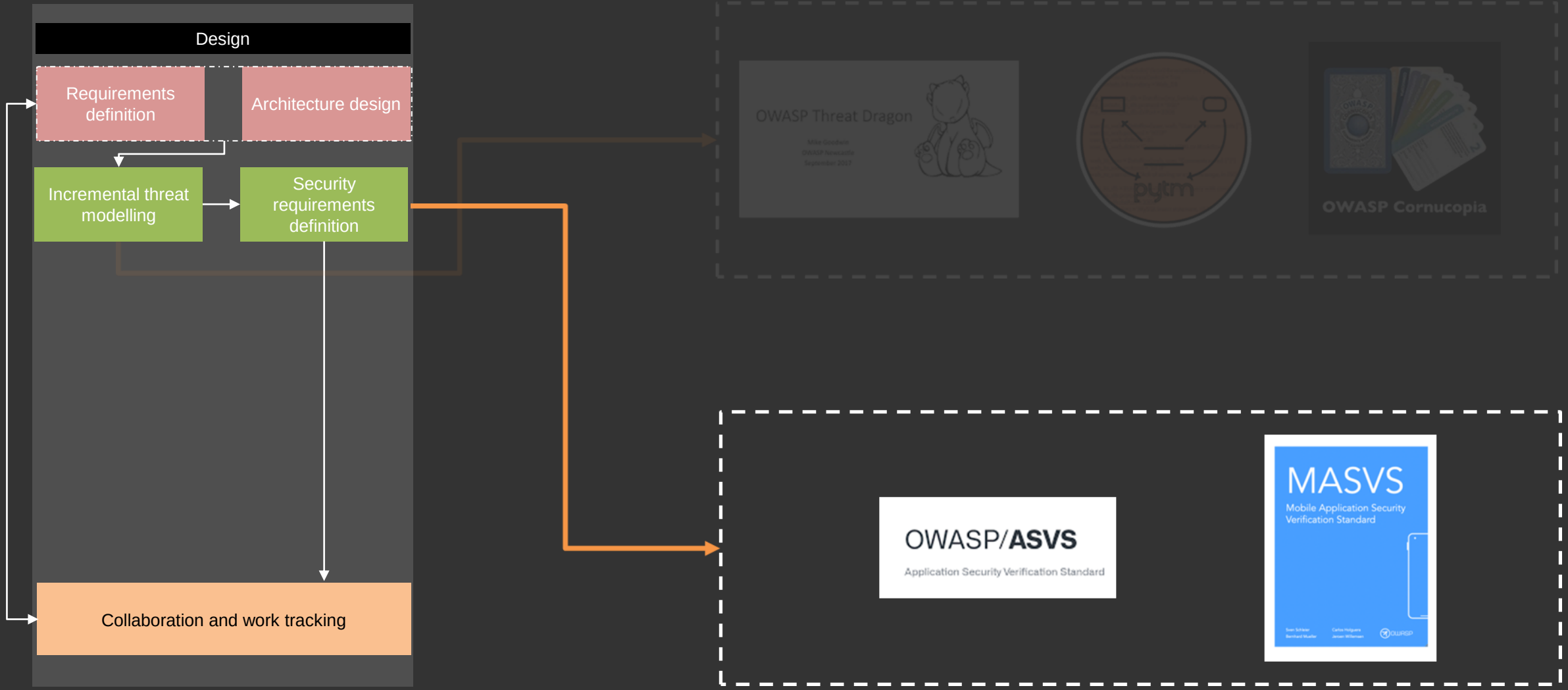
OWASP Secure Coding Practices Quick Reference Guide

OWASP Cheat Sheet Series

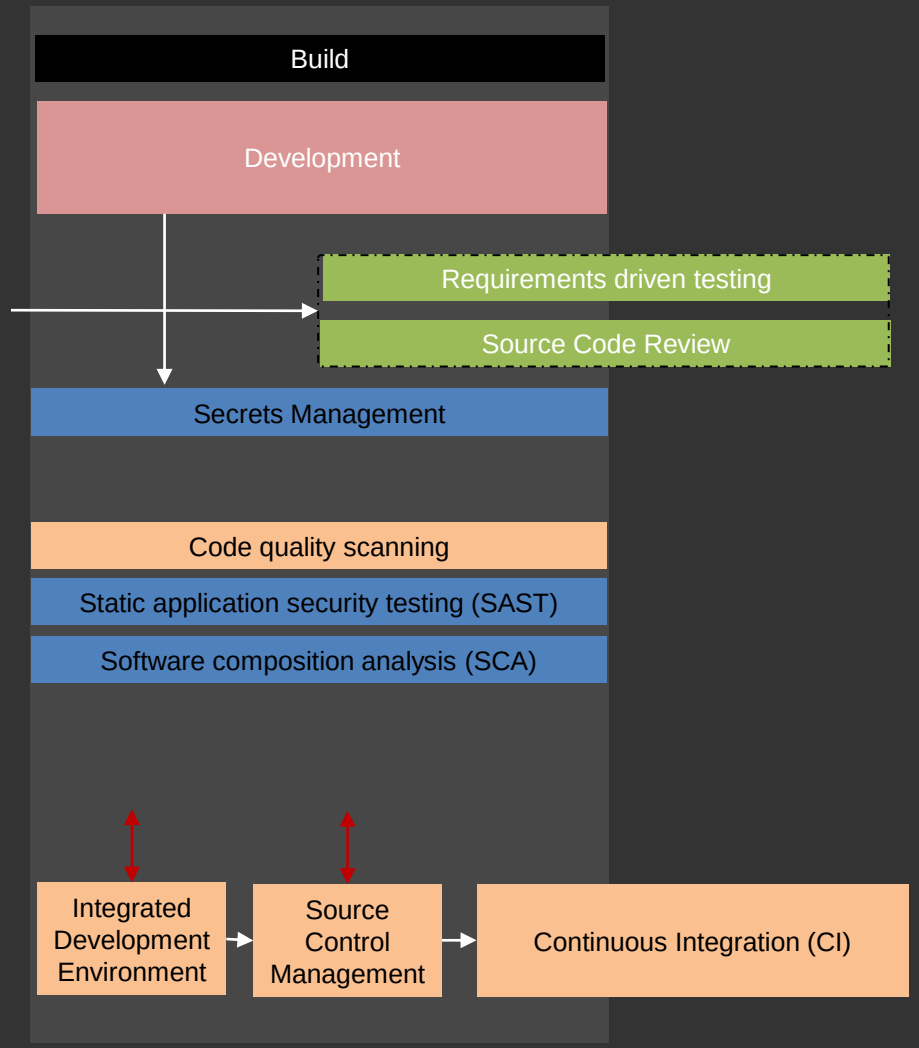
Design

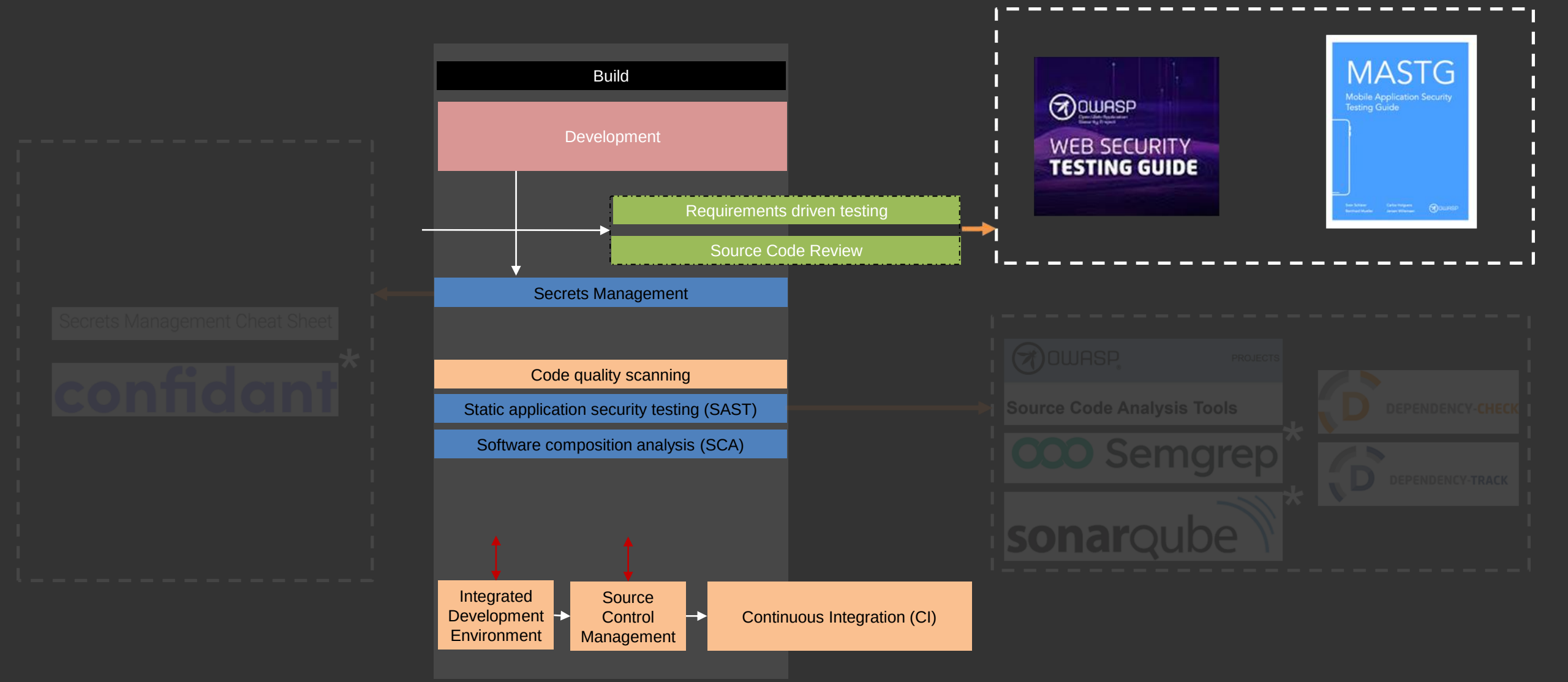

Design
Requirements definition
Architecture design
Incremental threat modelling
Security requirements definition
Collaboration and work tracking


Design
Requirements definition
Architecture design
Incremental threat modelling
Security requirements definition
Collaboration and work tracking
OWASP Threat Dragon
Mike Goodwin
OWASP Newcastle
September 2017
pytm
OWASP Cornucopia
OWASP/ASVS
Application Security Verification Standard
MASVS
Mobile Application Security Verification Standard

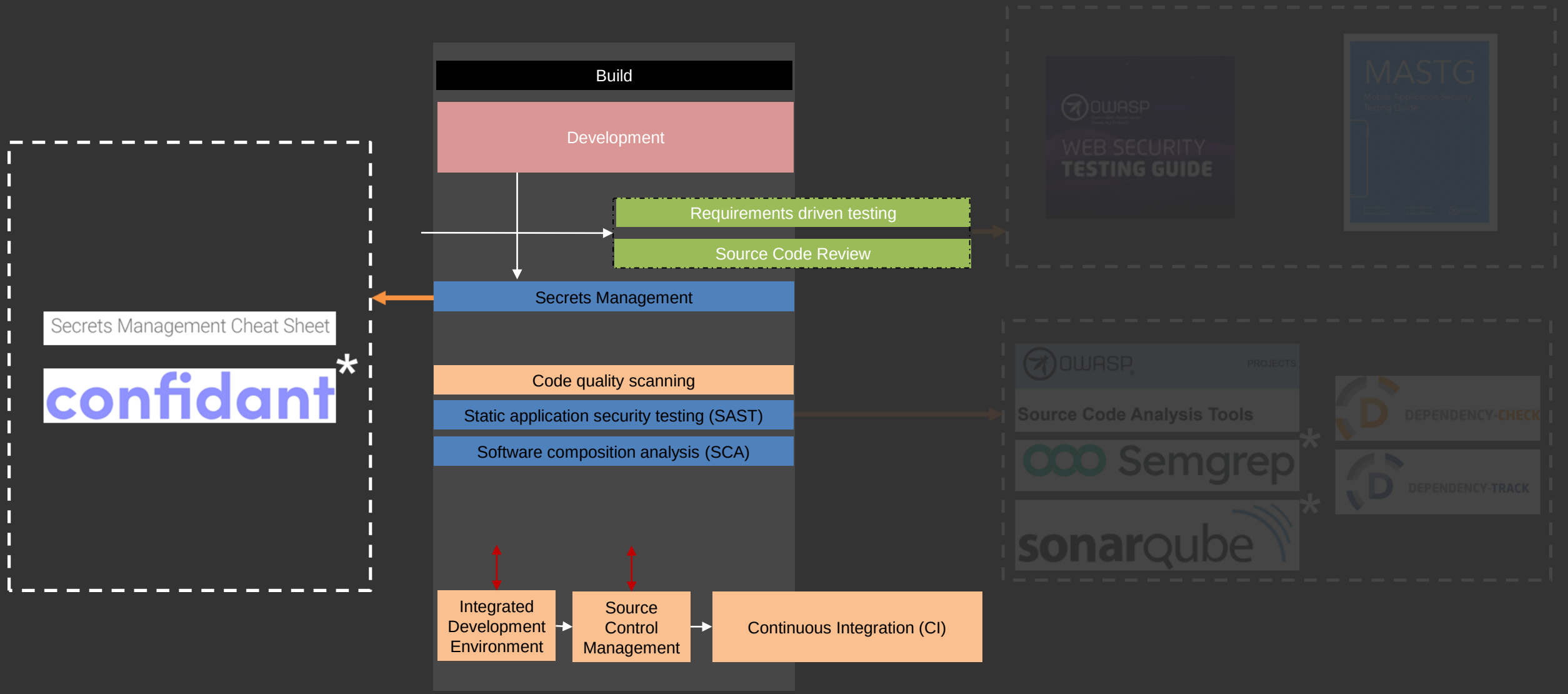

Design
Requirements definition
Architecture design
Incremental threat modelling
Security requirements definition
Collaboration and work tracking
OWASP Threat Dragon
pytm
OWASP Cornucopia
OWASP/ASVS
Application Security Verification Standard
MASVS
Mobile Application Security Verification Standard

Build

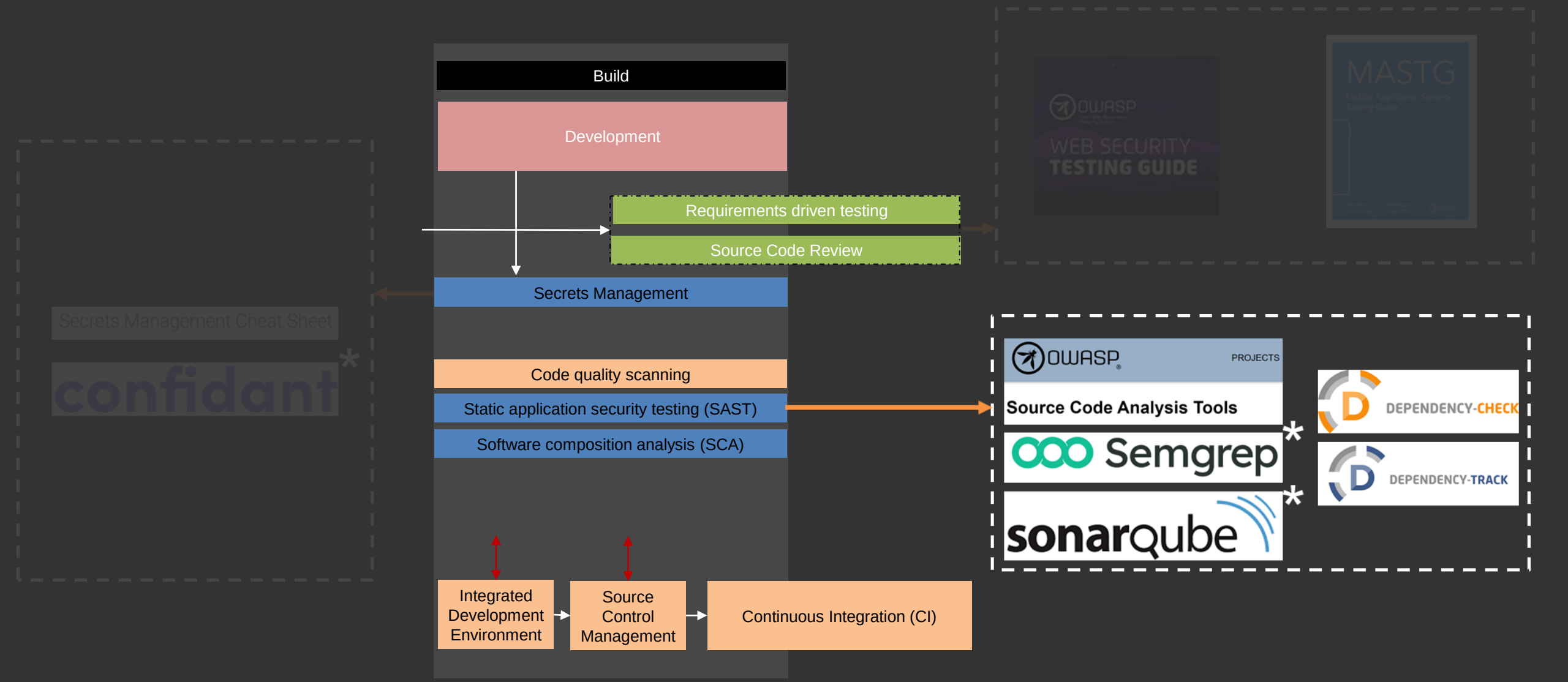

Build
Development
Requirements driven testing
Source Code Review
Secrets Management
Code quality scanning
Static application security testing (SAST)
Software composition analysis (SCA)
Integrated Development Environment
Source Control Management
Continuous Integration (CI)


Build
Development
Requirements driven testing
Source Code Review
Secrets Management
Code quality scanning
Static application security testing (SAST)
Software composition analysis (SCA)
Integrated Development Environment
Source Control Management
Continuous Integration (CI)
OWASP
WEB SECURITY TESTING GUIDE
MASTG
Mobile Application Security Testing Guide
Secrets Management Cheat Sheet
confidant
OWASP PROJECTS
Source Code Analysis Tools
Semgrep
sonarqube
DEPENDENCY-CHECK
DEPENDENCY-TRACK

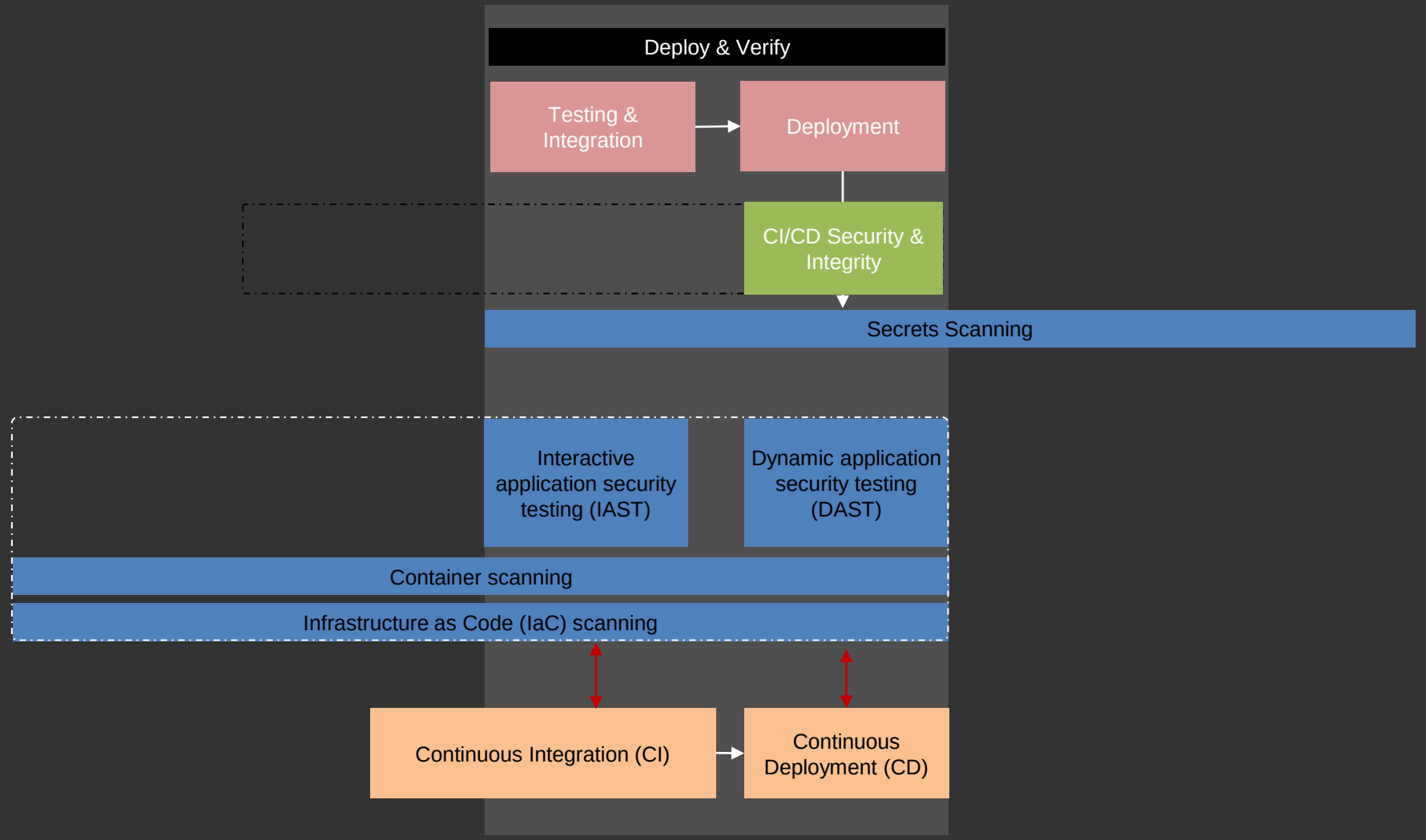
*Not an OWASP project/tool



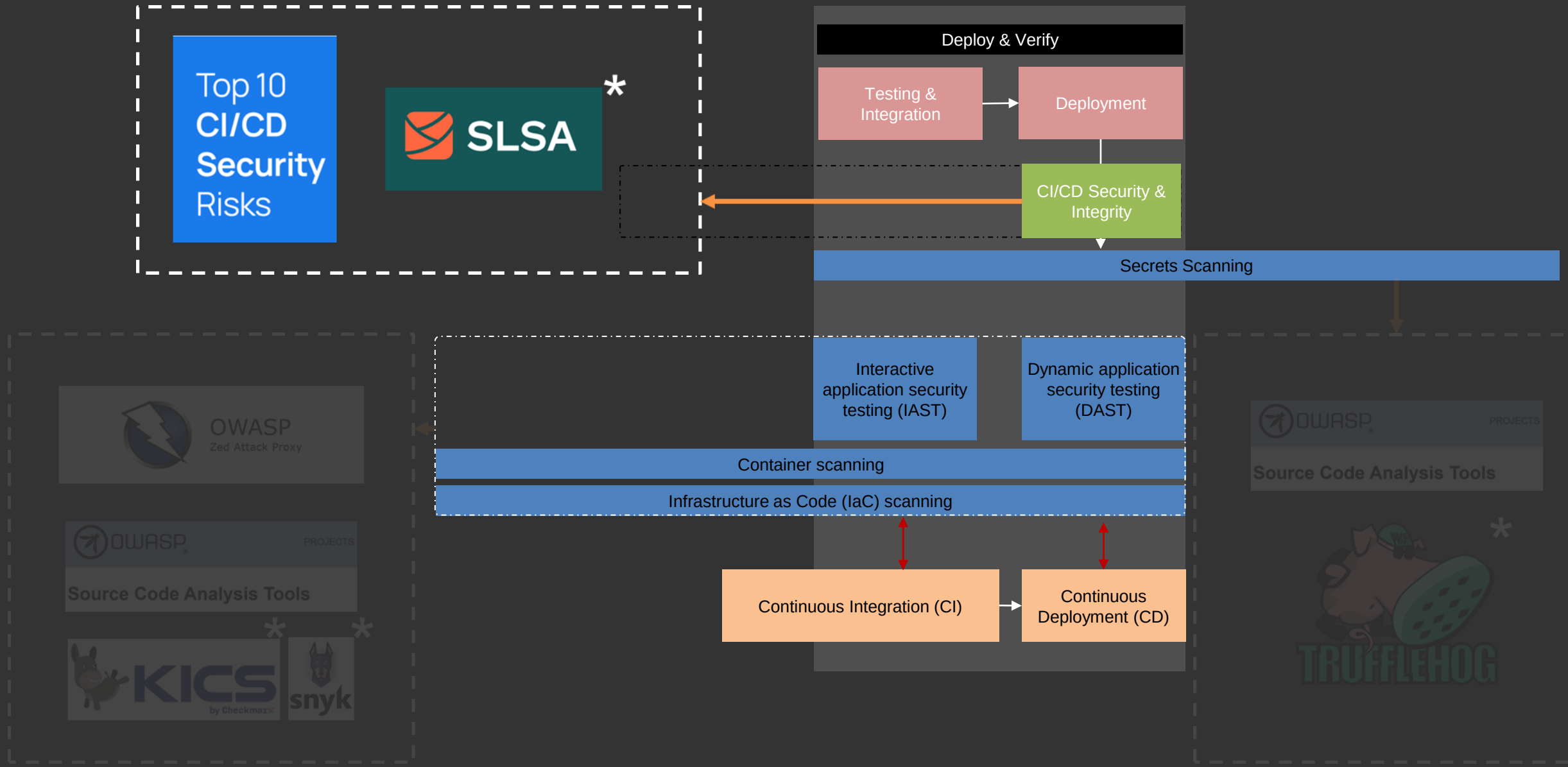
*Not an OWASP project/tool



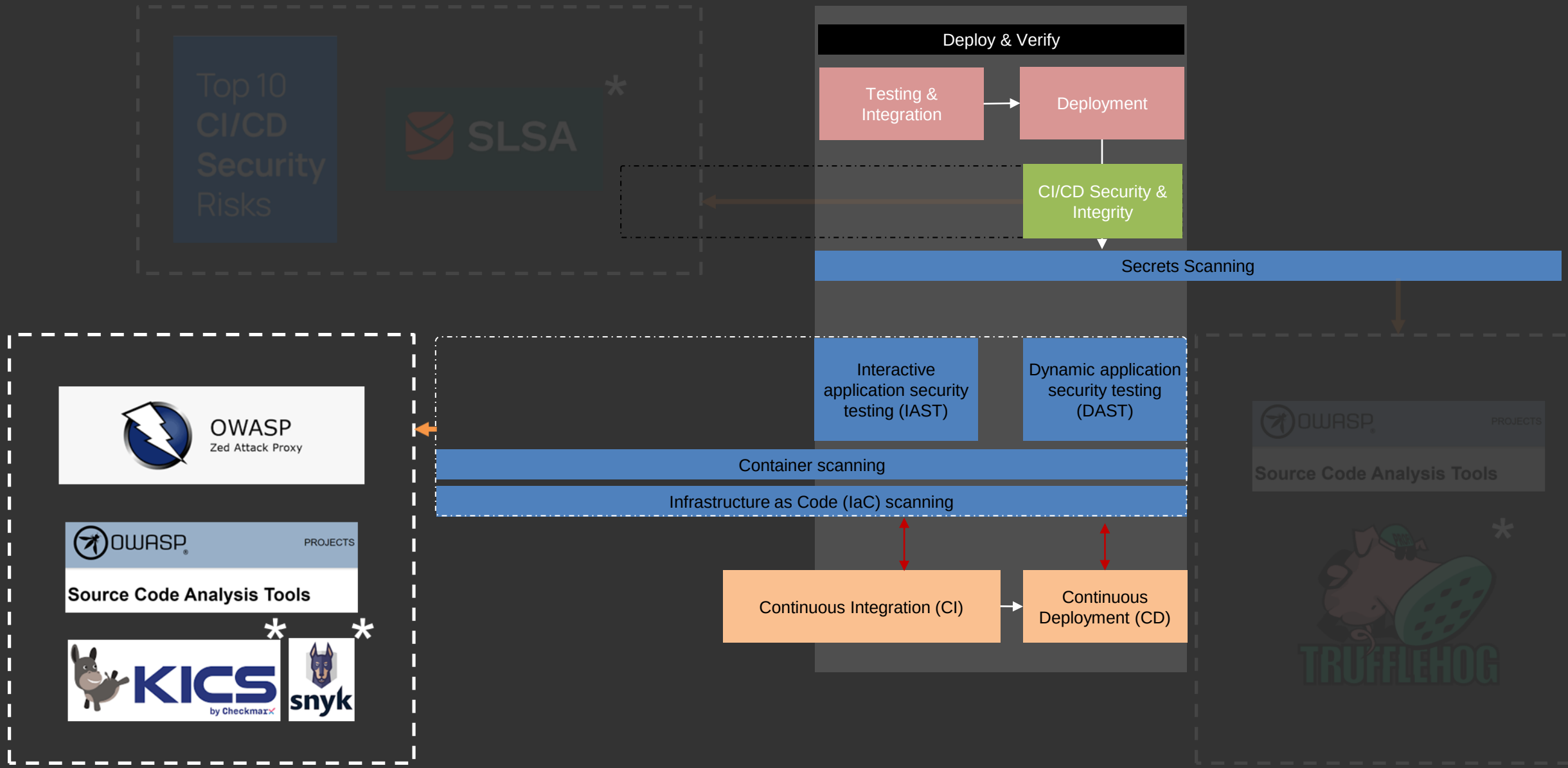
Deploy and Verify


Deploy & Verify
Testing & Integration
Deployment
CI/CD Security & Integrity
Secrets Scanning
Interactive application security testing (IAST)
Dynamic application security testing (DAST)
Container scanning
Infrastructure as Code (IaC) scanning
Continuous Integration (CI)
Continuous Deployment (CD)

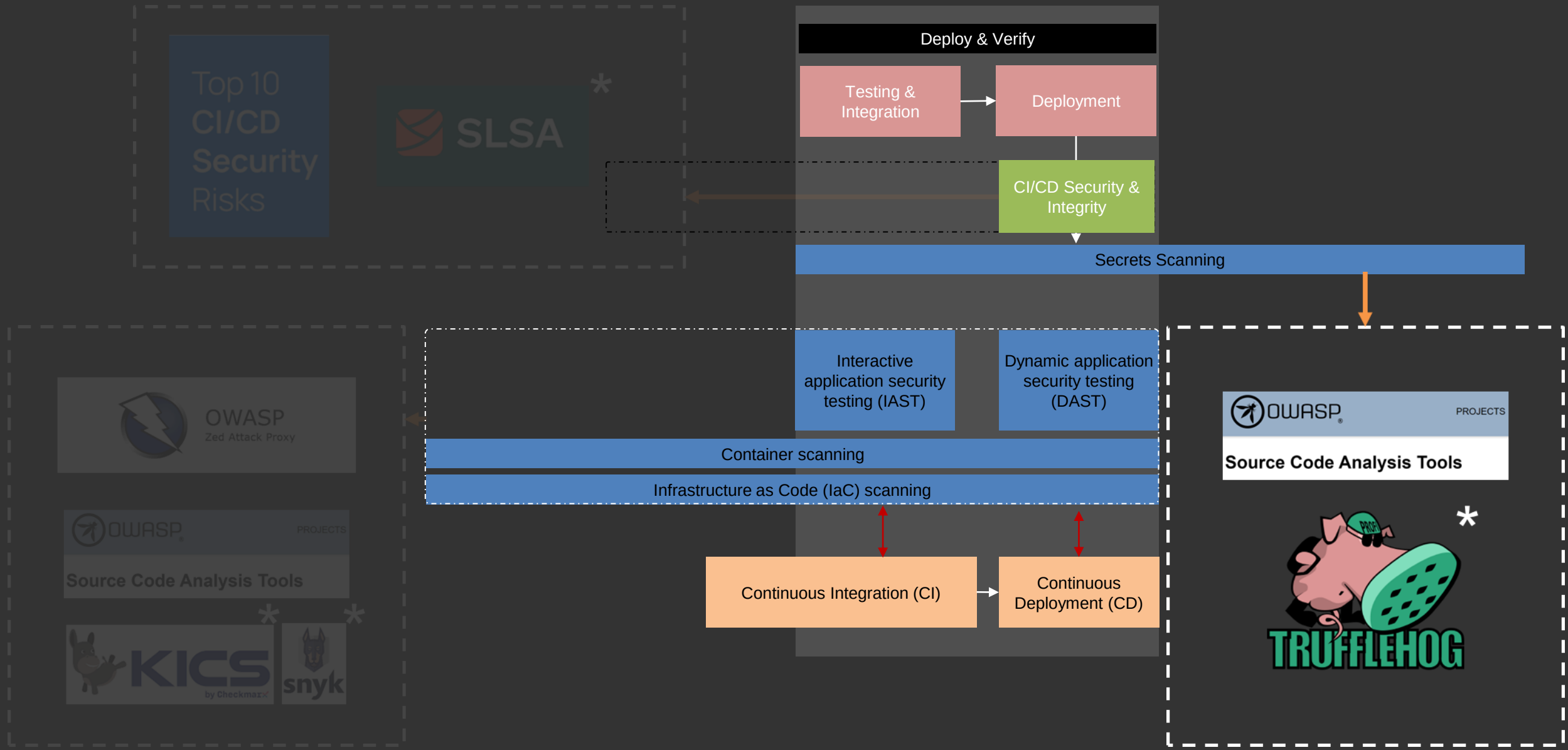
*Not an OWASP project/tool



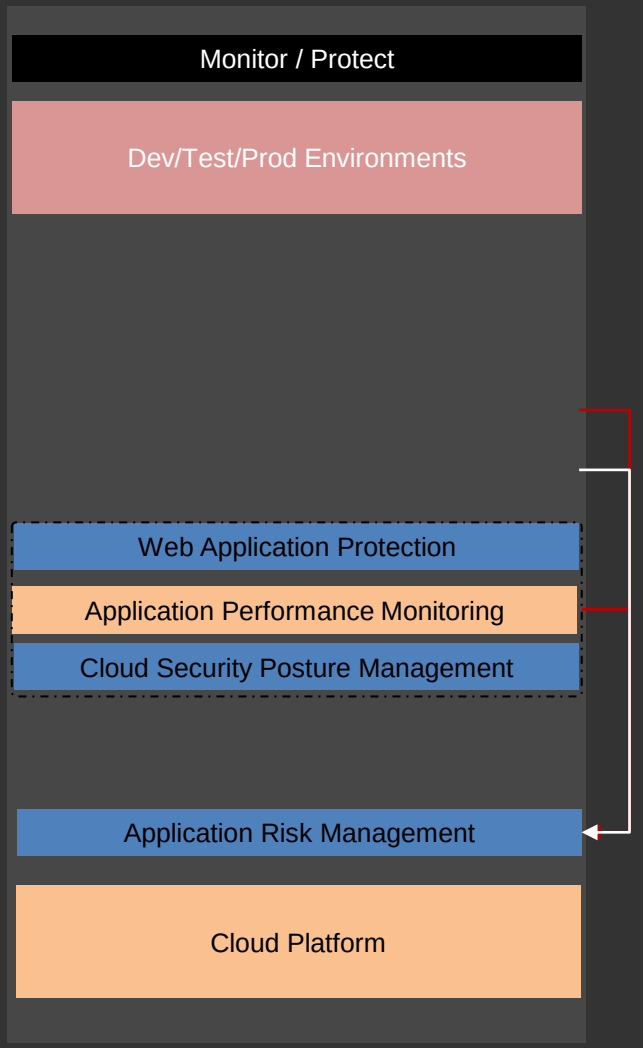
*Not an OWASP project/tool



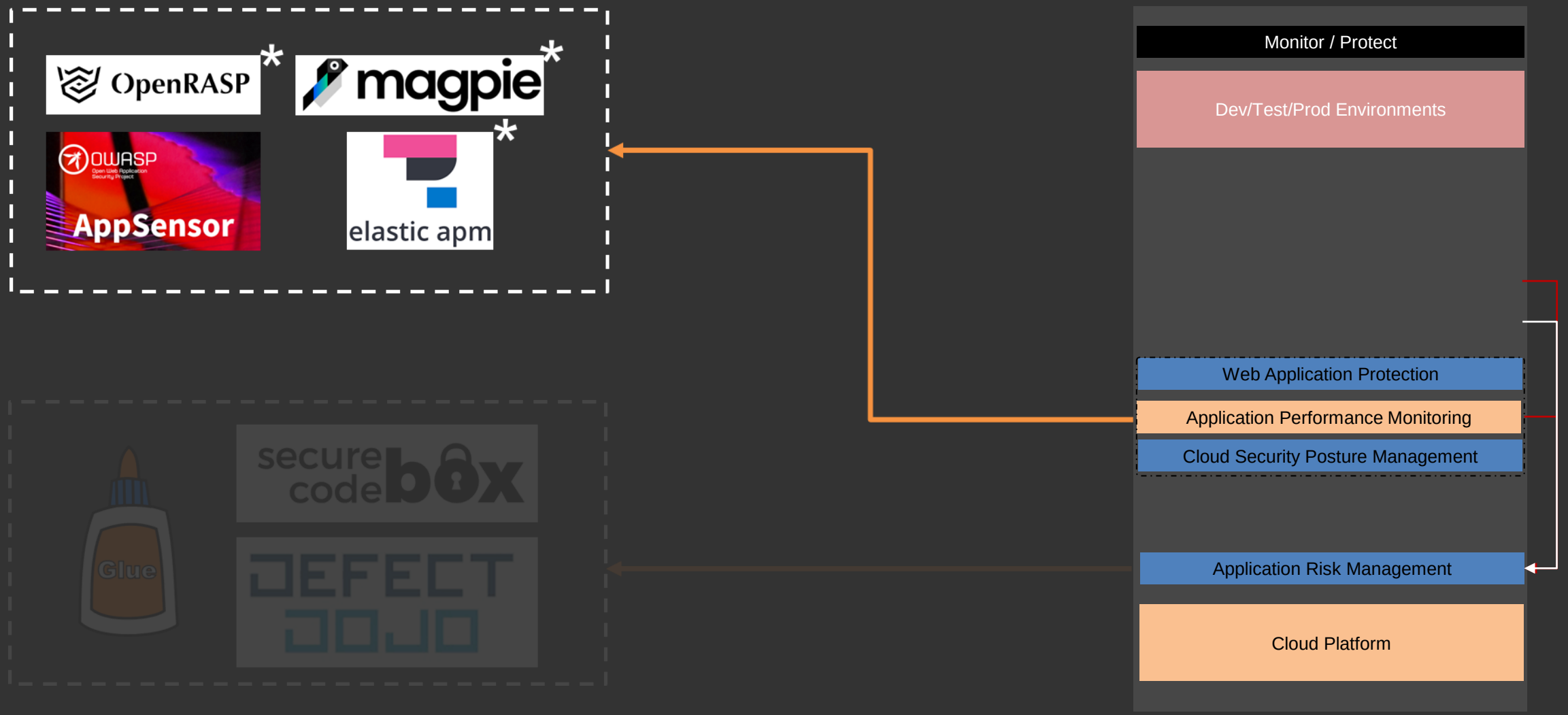
*Not an OWASP project/tool



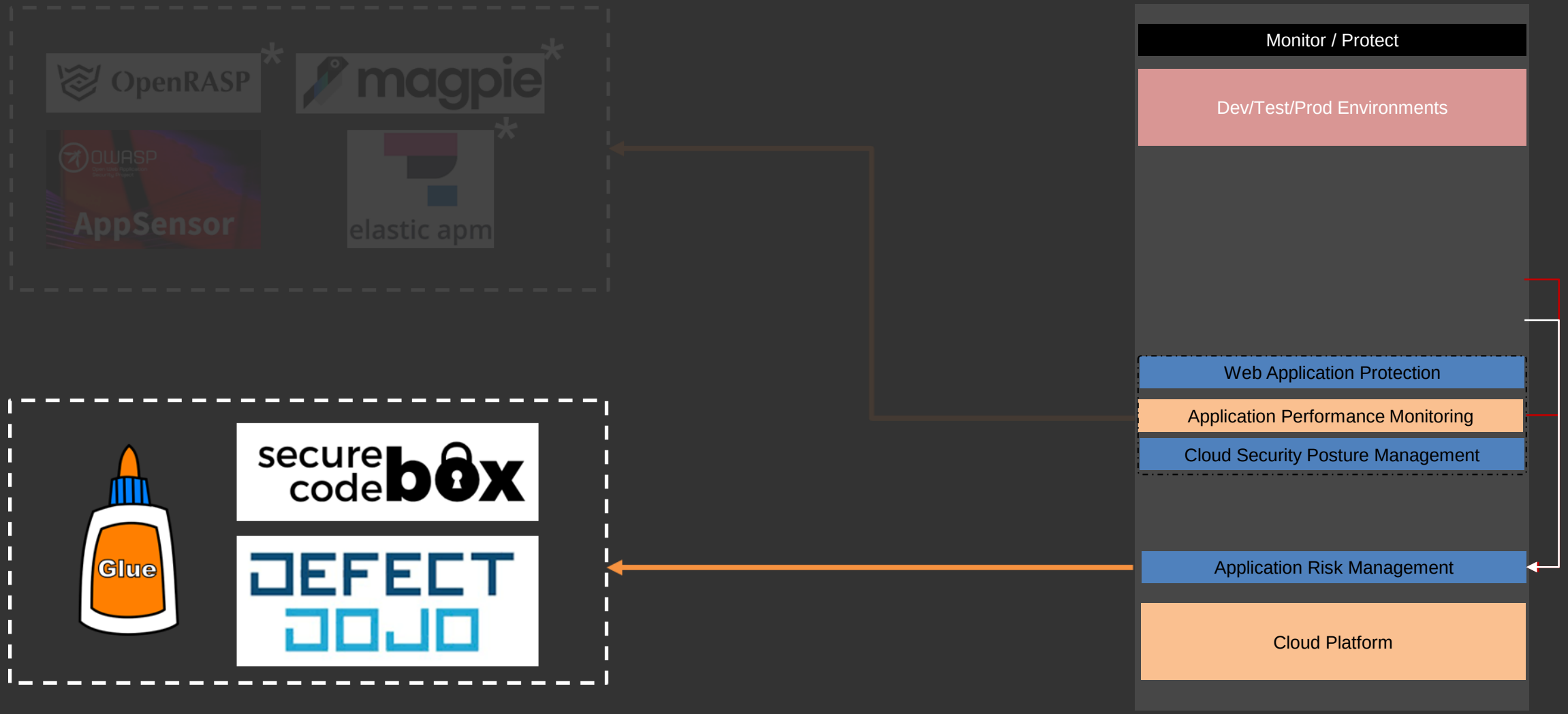
Monitor & Protect


Monitor / Protect
Dev/Test/Prod Environments
Web Application Protection
Application Performance Monitoring
Cloud Security Posture Management
Application Risk Management
Cloud Platform

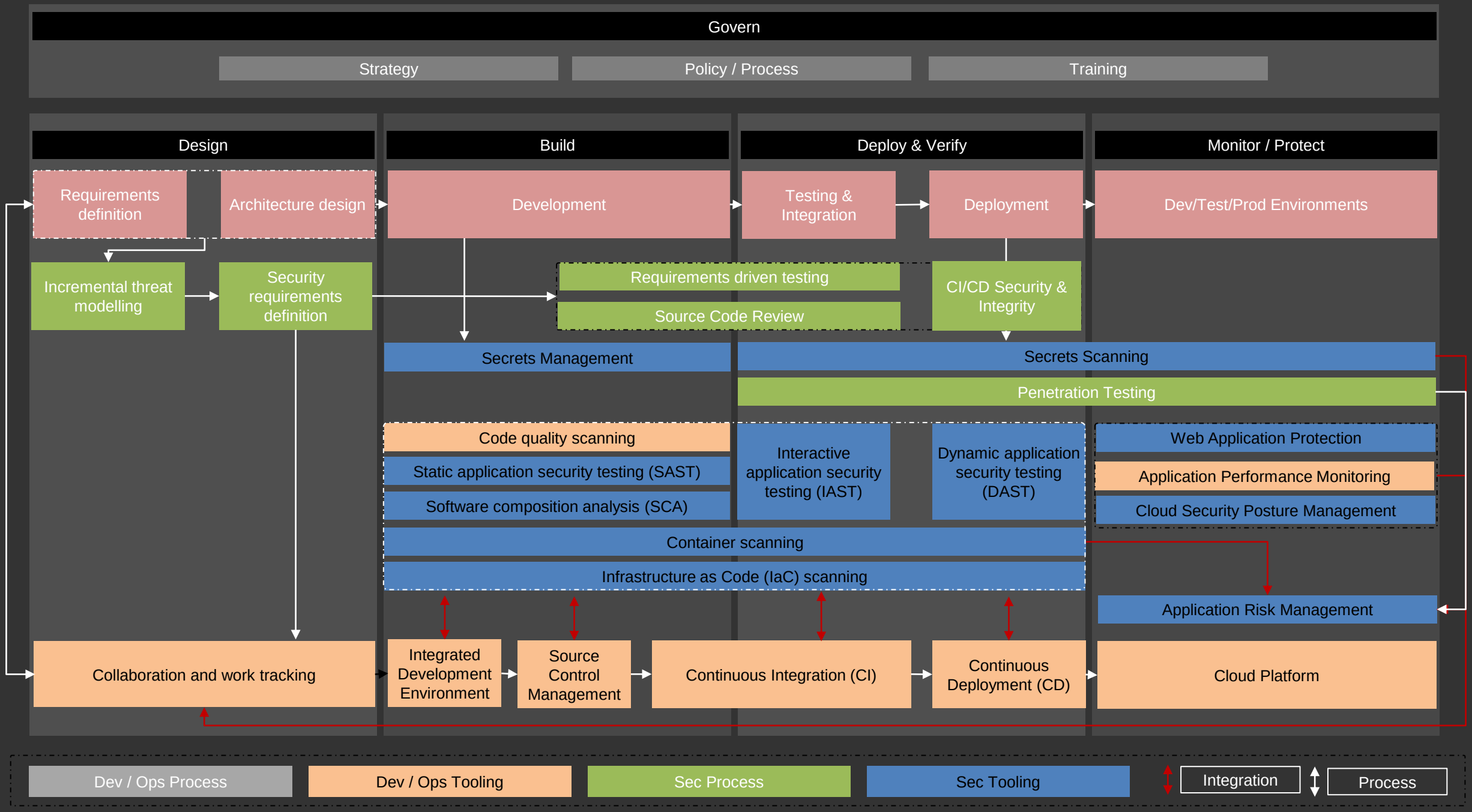
*Not an OWASP project/tool

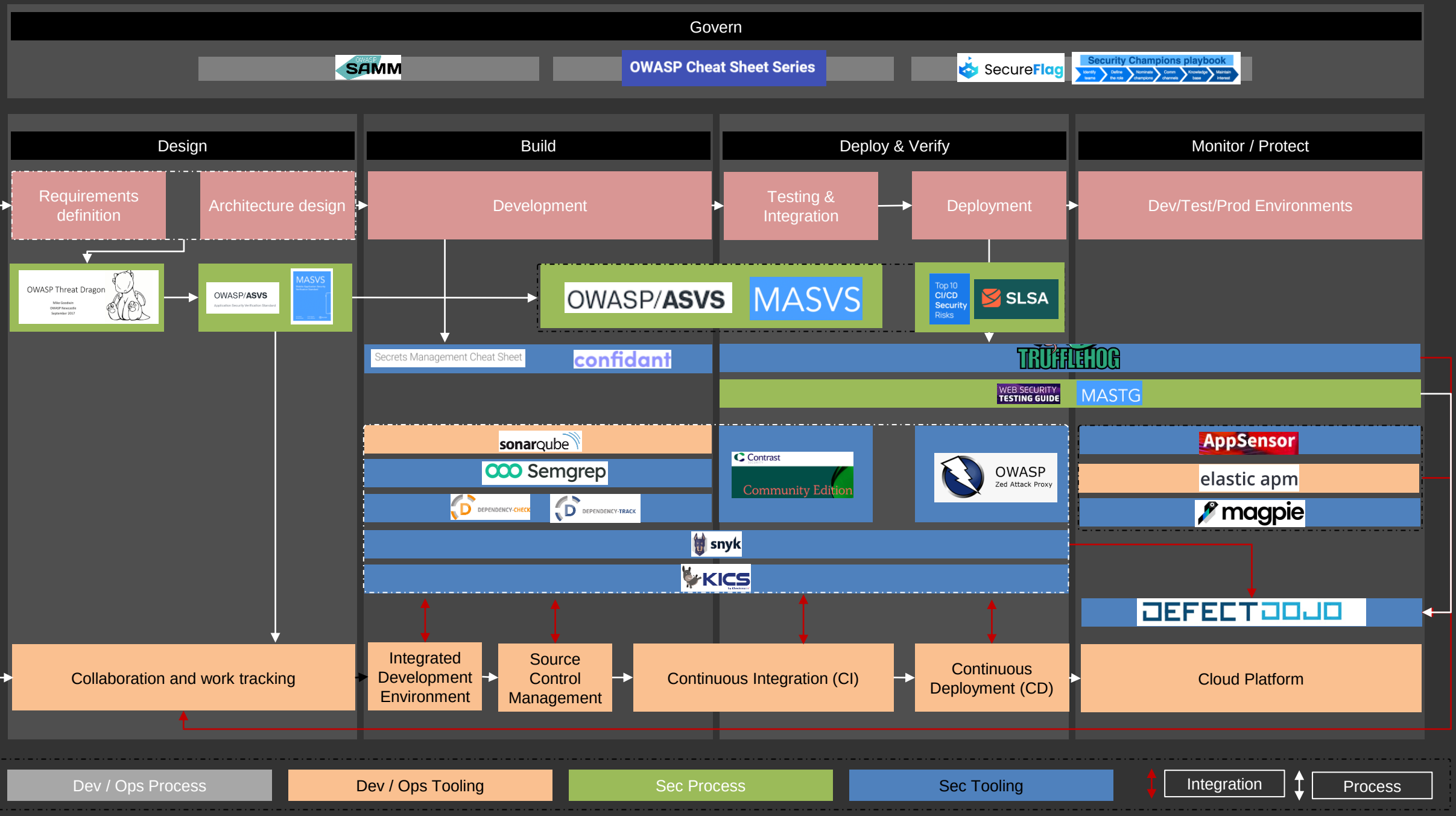


*Not an OWASP project/tool



All Together Now


Govern
Strategy
Policy / Process
Training
Design
Build
Deploy & Verify
Monitor / Protect
Requirements definition
Architecture design
Development
Testing & Integration
Deployment
Dev/Test/Prod Environments
Incremental threat modelling
Security requirements definition
Requirements driven testing
Source Code Review
CI/CD Security & Integrity
Secrets Management
Secrets Scanning
Penetration Testing
Code quality scanning
Static application security testing (SAST)
Software composition analysis (SCA)
Interactive application security testing (IAST)
Dynamic application security testing (DAST)
Web Application Protection
Application Performance Monitoring
Cloud Security Posture Management
Container scanning
Infrastructure as Code (IaC) scanning
Application Risk Management
Collaboration and work tracking
Integrated Development Environment
Source Control Management
Continuous Integration (CI)
Continuous Deployment (CD)
Cloud Platform
Dev / Ops Process
Dev / Ops Tooling
Sec Process
Sec Tooling
Integration
Process


Govern
OWASP SAMM
OWASP Cheat Sheet Series
SecureFlag
Security Champions playbook
Design
Build
Deploy & Verify
Monitor / Protect
Requirements definition
Architecture design
Development
Testing & Integration
Deployment
Dev/Test/Prod Environments
OWASP Threat Dragon
OWASP/ASVS
MASVS
OWASP/ASVS
MASVS
Top 10 CI/CD Security Risks
SLSA
Secrets Management Cheat Sheet
confidant
TRUFFLEHOG
WEB SECURITY TESTING GUIDE
MASTG
sonarqube
Semgrep
DEPENDENCY-CHECK
DEPENDENCY-TRACK
Contrast
Community Edition
OWASP
Zed Attack Proxy
AppSensor
elastic apm
magpie
snyk
KICS
DEFECTDOJO
Collaboration and work tracking
Integrated Development Environment
Source Control Management
Continuous Integration (CI)
Continuous Deployment (CD)
Cloud Platform
Dev / Ops Process
Dev / Ops Tooling
Sec Process
Sec Tooling
Integration
Process

Now what?

Too many things

Figure out what's most important

~~Guidance often talks about what not how~~

There's quite a lot of guidance on how

Everyone solves "DevSecOps" now?

Try before you buy

Now what?

Too many things

Figure out what's most important

~~Guidance often talks about what not how~~

There's quite a lot of guidance on how

Everyone solves "DevSecOps" now?

Try before you buy

Now what?

Too many things

Figure out what's most important

~~Guidance often talks about what not how~~

There's quite a lot of guidance on how

Everyone solves "DevSecOps" now?

Try before you buy

Questions?

Reach me on:

- **OWASP Slack**
  Raafey
- **LinkedIn**
  Raafey Khan
- **Email**
  Raafey.khan@cybercx.com.au)