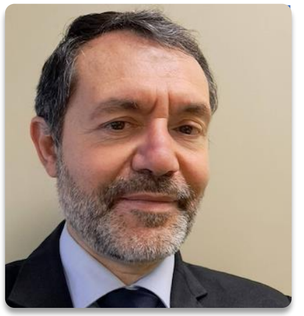
DevSecOps
...verso dove spostarsi ?

E. Trasatti | Resp. Soluzioni e Servizi di Sicurezza, *Sogei*

Enrico Trasatti

Responsabile Soluzioni e Servizi di Sicurezza di Sogei



Chi è Sogei?

In qualità di **partner tecnologico unico del Ministero dell'Economia e delle Finanze** sviluppa sistemi, applicazioni e servizi per tutte le esigenze di automazione e informatizzazione dei processi operativi e gestionali del Ministero, della Corte dei conti, delle Agenzie fiscali e di altre pubbliche amministrazioni.

Principali Clienti

Agenzia Entrate · ADM · Agenzia del Demanio · Agenzia Entrate-Riscossione · Corte dei Conti · MEF · Ministero dell'Interno · Ministero dell'Ambiente e della Tutela del Territorio e del Mare · MUR · Ministero della Giustizia · Ministero della Salute · Presidenza del Consiglio dei Ministri · ACN · MIM Ministero dell'Istruzione e del Merito · Equitalia Giustizia · Ministero della Cultura · consip

Di cosa mi occupo?

sogei

Cybersecurity

Soluzioni e Servizi di Sicurezza

- Red Teaming & Penetration Test
- Vulnerability Assessment & Management
- Cloud & Container Security
- DevSecOps

Uno Scenario Operativo complesso …

sogei

20+
Domini Applicativi

10.000+
Rilasci Annuali

1500+
Sviluppatori

5000+
Repository

Eterogeneità Linguaggi utilizzati:

Java

Javascript

.NET

…

500+
Servizi web erogati

Ambito Deploy:

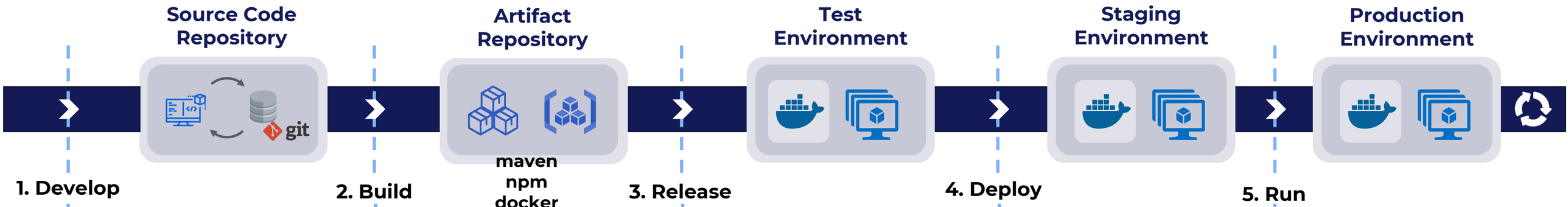
Legacy & Microservizi

40M+
Linee di codice sviluppate

La Teoria

Processo Generale SDLC

DevOps



1

Fase in cui il **codice sorgente** viene creato dai team di sviluppo. L'output è conservato nel **Source Code Repository**, che **gestisce** e **traccia** tutte le **versioni** e **modifiche**

2

Fase di **compilazione** e **packaging** del software. Gli **artefatti** generati vengono depositati **nell'Artifact Repository**, pronti per la distribuzione.

3

Fase in cui l'**applicazione** viene **rilasciata** e distribuita nel **Test Environment**. In questo ambiente si verifica la **qualità** del software con **appositi test funzionali e non**.

4

Fase di **deploy** nell' **ambiente di staging** per eseguire il **collaudo** finale prima del passaggio in produzione.

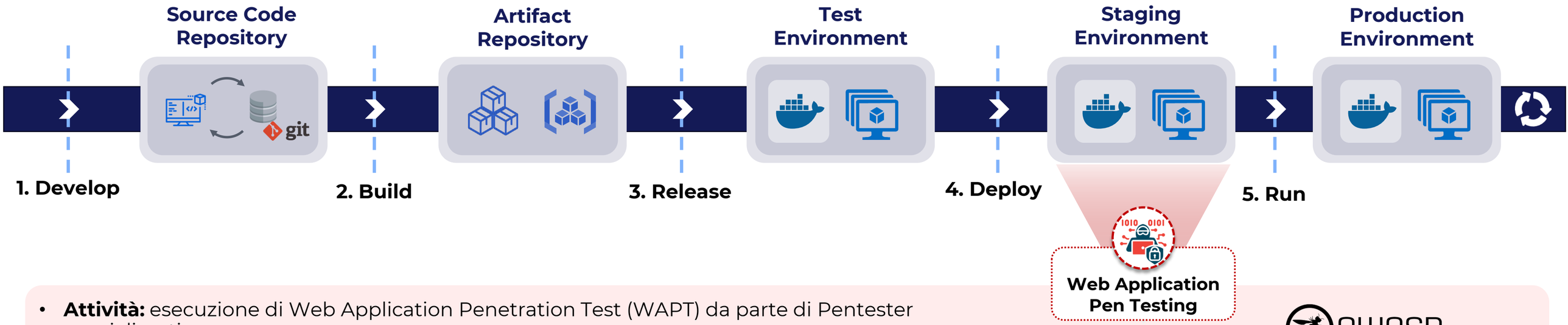
5

Fase **operativa** in cui l'applicazione passa in **produzione** e il servizio è erogato agli **utenti finali**

La Teoria

Esecuzione WAPT nel processo SDLC

DevOps



- **Attività:** esecuzione di Web Application Penetration Test (WAPT) da parte di Pentester specializzati.
- **Classificazione di riferimento:** OWASP TOP 10 2021

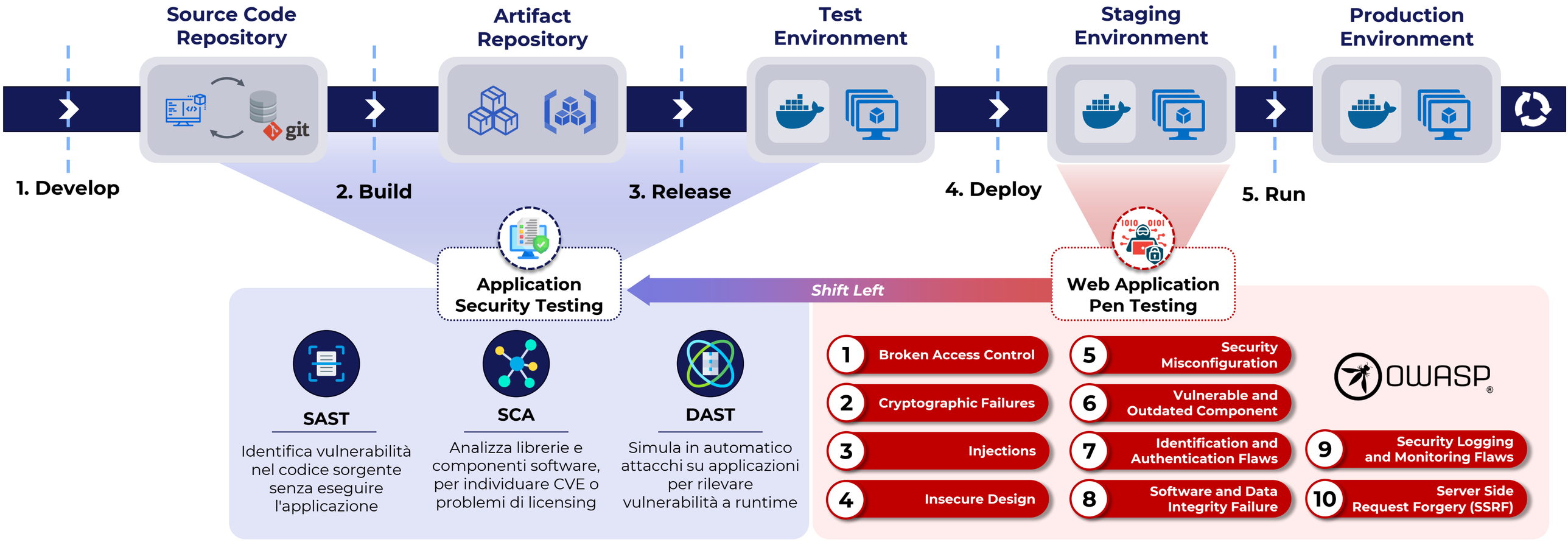
OWASP®

1 Broken Access Control	3 Injections
2 Cryptographic Failures	4 Insecure Design
5 Security Misconfiguration	7 Identification and Authentication Flaws
6 Vulnerable and Outdated Component	8 Software and Data Integrity Failure
9 Security Logging and Monitoring Flaws	10 Server Side Request Forgery (SSRF)

La Teoria

Inserimento di controlli automatici AST nel SDLC

DevSecOps



La Pratica

... alcune questioni da affrontare e risolvere

Key Questions:

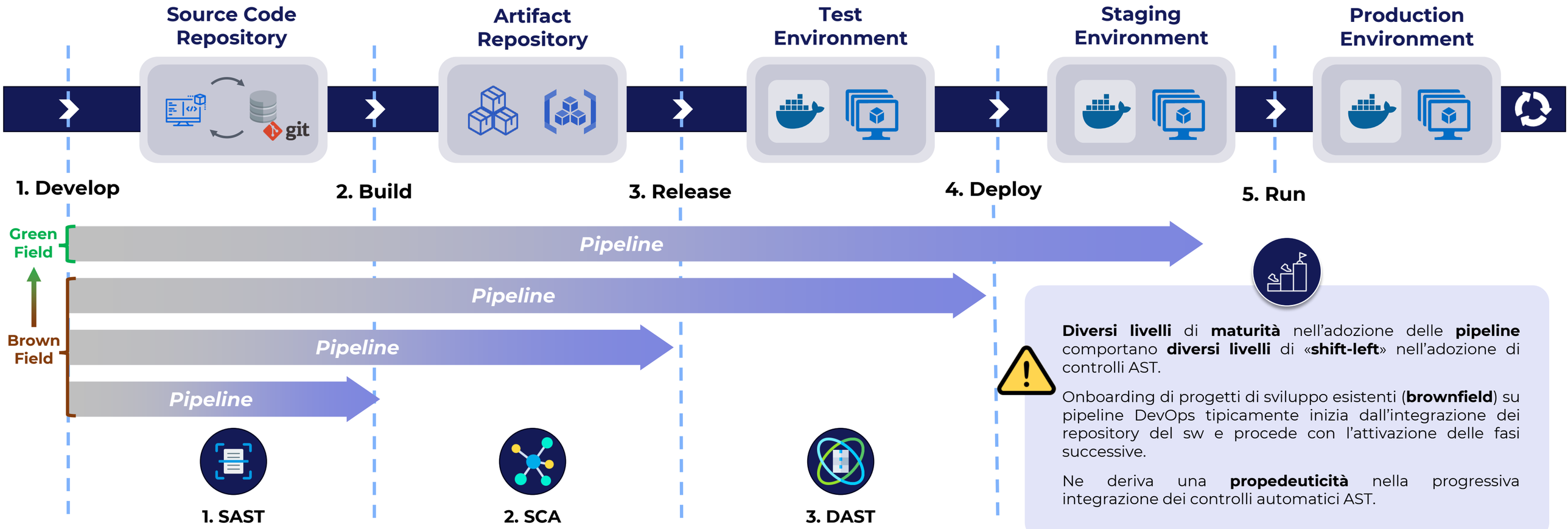
1. In ottica di **onboarding progressivo** da **quali controlli** conviene **iniziare** e perché?
2. **Applicando** controlli automatici di tipo **SAST**, **SCA** e **DAST/IAST** abbiamo lo **stesso** tipo di **copertura** dei **WAPT** manuali, riservandoli solo per situazioni particolari?
3. Se ci fossero **vulnerabilità** per loro natura **non** facilmente **individuabili** da controlli **automatici**, **come indirizzarle** e prevenirle nel SDLC?
4. **Come coinvolgere** in modo efficace i **team** di **sviluppo**?
5. **Come assicurarsi** infine che ciò che va in **produzione** abbia effettivamente **superato tutti** i **controlli**, mentre ci saranno molti altri componenti sw in fase di sviluppo con vulnerabilità da risolvere?
6. **Come gestire** nel SDLC le **vulnerabilità** che emergono "**unattended**" **dopo** aver messo in **esercizio** il **codice**? (es. CVE delle librerie)

Aspetti da **trattare** con particolare **attenzione** ed **effort**

La Pratica

Inserimento controlli AST nel SDLC … propedeuticità

DevSecOps



Diversi livelli di **maturità** nell'adozione delle **pipeline** comportano **diversi livelli** di «**shift-left**» nell'adozione di controlli AST.

Onboarding di progetti di sviluppo esistenti (**brownfield**) su pipeline DevOps tipicamente inizia dall'integrazione dei repository del sw e procede con l'attivazione delle fasi successive.

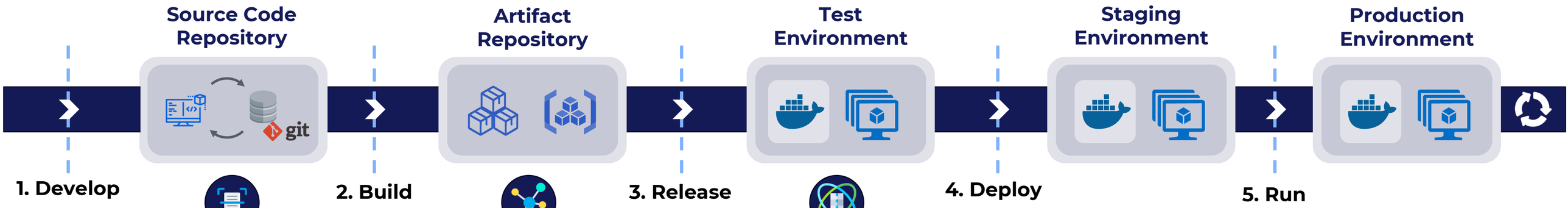
Ne deriva una **propedeuticità** nella progressiva integrazione dei controlli automatici AST.

Aspetti da **trattare** con particolare **attenzione** ed **effort**

La Pratica

Inserimento controlli AST nel SDLC … propedeuticità

DevSecOps



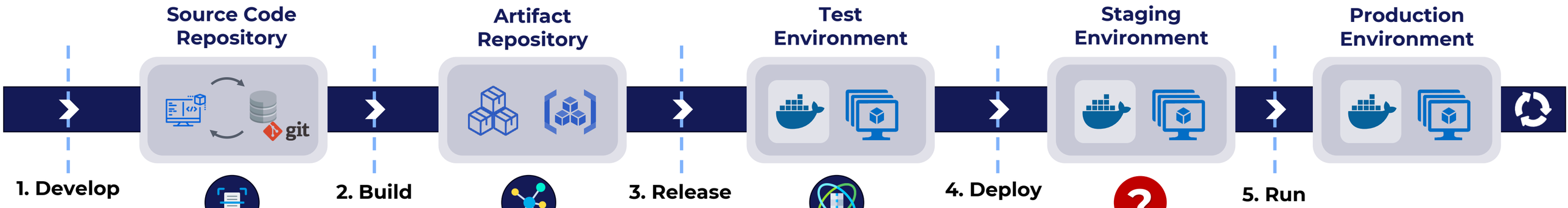
	SAST	SCA	DAST
Benefici	▶ **Maggiore copertura** dei **progetti** ▶ **Indicazioni utili** allo **sviluppatore** sul codice	▶ **Semplicità** d'**integrazione** nel SDLC ▶ **Chiarezza** della **segnalazione** e del **tipo** di **intervento** da **eseguire**	▶ **Copertura vulnerabilità** e **pochi falsi positivi** ▶ Chiarezza della **gravità** della **vulnerabilità** e dell'**exploit** ▶ Verifica **superficie esposta**
Effort Richiesto	▶ **Necessità** di **formazione** su vulnerabilità **OWASP** ▶ **Maggior** numero di **potenziali falsi positivi** ▶ **Tuning** degli **strumenti** e **ruoli specifici** nei **team** di **Dev**	▶ **Pianificazione** a **medio-lungo termine** per **update** librerie ▶ **Gestione** di **interdipendenze** tra i **team** di **Dev** ▶ Integrazione **SCA** – **Container Security**	▶ **Training** del **team** di **Dev** per l'**utilizzo** dei tool **DAST** ▶ **Registrazione navigazione** per la **completezza** dei **test** sulle funzionalità sviluppate

Aspetti da **trattare** con particolare **attenzione** ed **effort**

La Pratica

Quali vulnerabilità individuabili con quali controlli AST...

DevSecOps



SAST

- 2 Cryptographic Failures
- 3 Injections
- 7 Identification and Authentication Flaws
- 9 Security Logging and Monitoring Flaws

SCA

- 6 Vulnerable and Outdated Component
- 8 Software and Data Integrity Failure

DAST

- 2 Cryptographic Failures
- 3 Injections
- 5 Security Misconfiguration
- 6 Vulnerable and Outdated Component
- 7 Identification and Authentication Flaws
- 10 Server Side Request Forgery (SSRF)

WAPT

- 1 Broken Access Control
- 4 Insecure Design

Shift Left

Alcune classi di vulnerabilità, che dipendono dalla **logica di business** e **autorizzativa** dell'applicazione, potrebbero non essere rilevabili dalle analisi automatiche ma essere individuabili solo da Pentest manuali.

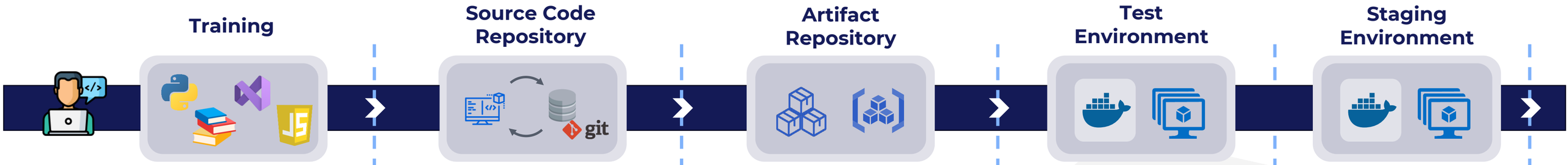
Una **formazione** dei team focalizzata su **sviluppo sicuro** e su **best practice di sicurezza** permette di mitigare in modo efficace i rischi a cui sono esposte le applicazioni.

Aspetti da **trattare** con particolare **attenzione** ed **effort**

La Pratica

… e vulnerabilità da prevenire con training e con test funzionali di sicurezza

SecDevOps



Focus prioritario

1 Broken Access Control

4 Insecure Design

+

OWASP® TOP 10 2021

SAST

2 Cryptographic Failures

3 Injections

7 Identification and Authentication Flaws

9 Security Logging and Monitoring Flaws

SCA

6 Vulnerable and Outdated Component

8 Software and Data Integrity Failure

DAST

2 Cryptographic Failures

3 Injections

5 Security Misconfiguration

6 Vulnerable and Outdated Component

7 Identification and Authentication Flaws

10 Server Side Request Forgery (SSRF)

"Test Funzionali" di sicurezza

1 Broken Access Control

4 Insecure Design

Predisporre **test dedicati** ai **controlli autorizzativi** e di **logica dell'applicazione** aumenta il livello di attenzione del team di sviluppo su questi aspetti.

Aspetti da **trattare** con particolare **attenzione** ed **effort**

La Pratica

Il training come «change» che va continuamente supportato

Iniziative progressive di training realizzate per team di sviluppo

1. Pubblicazione di linee guida
2. Sezione intranet
3. Community (canali, blog) per comunicazione interattiva
4. Webinar online
5. Piattaforme online con micro-laboratori virtuali
6. Percorsi di formazione definiti per ruolo (PM, SC o developer), per linguaggio, per tematica di sicurezza
7. Secure Coding Academy con iscrizione annuale, istruttori con programma di webinar live, esercitazioni di gruppo, challange iniziale e finale
8. Dashboard per verificare lo «score» di sicurezza raggiunto dai propri progetti in fase di sviluppo

Aspetti da **trattare** con particolare **attenzione** ed **effort**

La Pratica

i Security Champions, elementi chiave nel processo di «shift-left» e di «change»

Figure specialistiche integrate nei team di sviluppo

Operatività limitata all'essenziale

Dotati di tutti gli strumenti necessari, semplici per quanto possibile

Security Champions

100+ SC

Tutta la formazione e il supporto possibile a disposizione

Ufficialità del ruolo e designazione formale

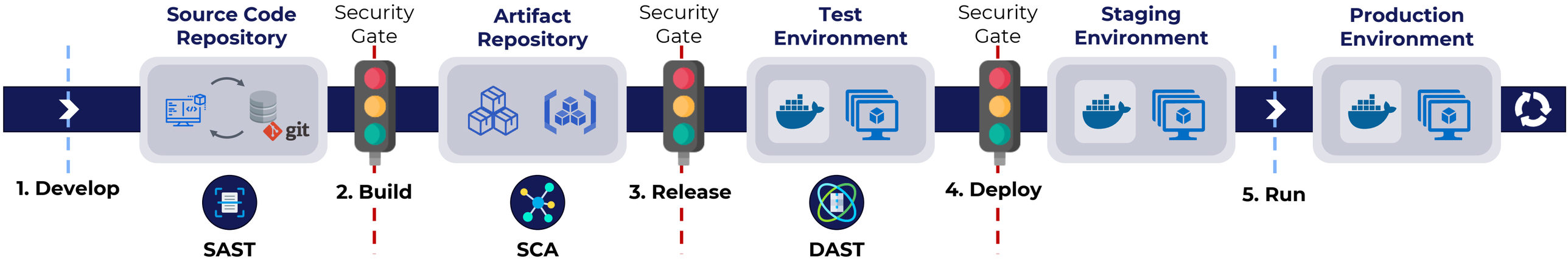
Costituzione di una Community registrata aziendalmente, riconosciuta come formazione specialistica

Aspetti da **trattare** con particolare **attenzione** ed **effort**

La Pratica

Attivare Security Gate in pipeline è possibile...

SecDevOps



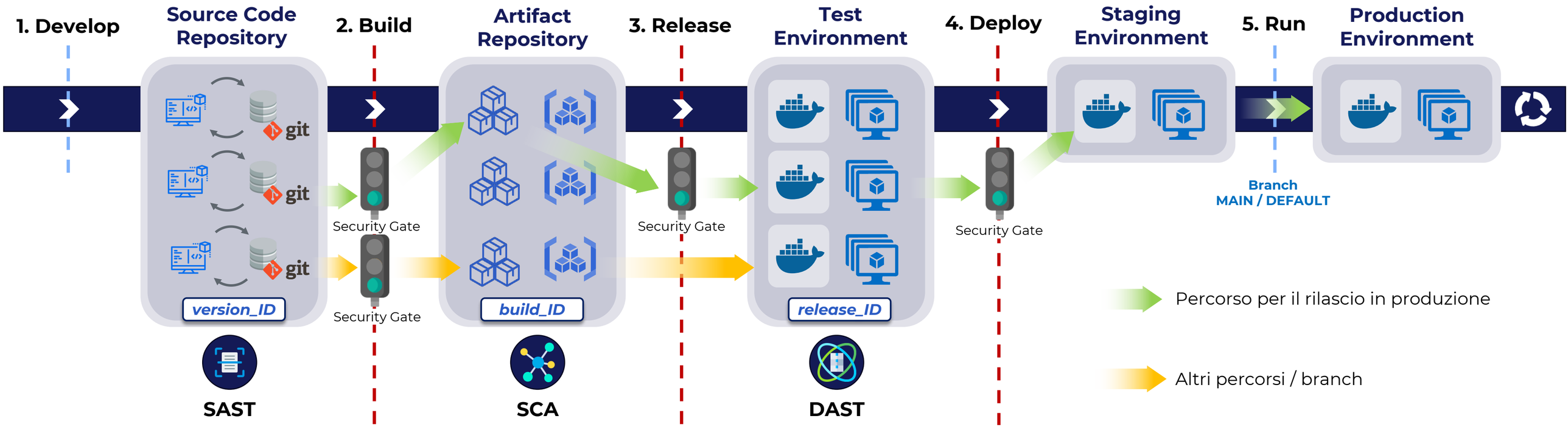
- Definire per ogni item l'identificativo da associare all'esito del controllo (SCA, SAST, DAST)
- Ogni fase deve avere un security gate da superare con soglia per specifico controllo definita in modo omogeneo alle altre

Controllo	Identificativo	Oggetto del controllo	Ambito del controllo
SAST	version_ID	Codice sorgente	Repository GIT
SCA	build_ID	Artefatti (image, .war, .jar, ...)	Repository artefatti
DAST	release_ID	URL, credenziali, dati test	Ambiente Test

Aspetti da **trattare** con particolare **attenzione** ed **effort**

La Pratica
… ma in quale ramo

SecDevOps



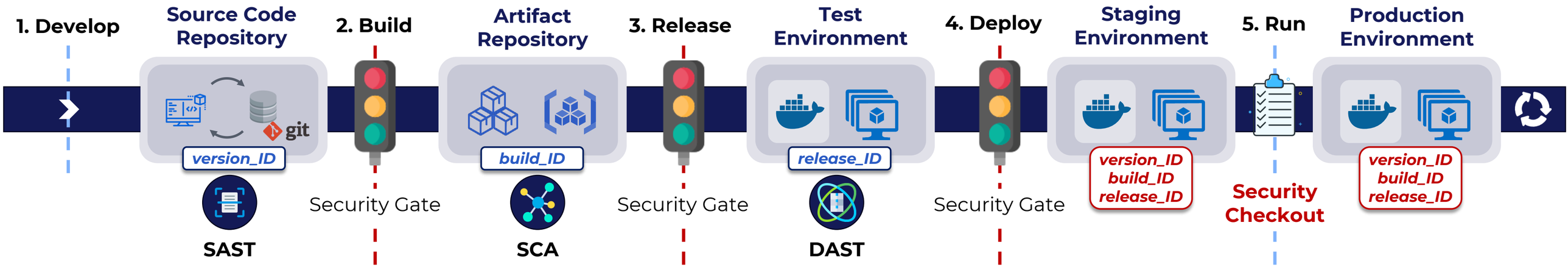
- Ci deve essere un **unico percorso** per arrivare alla **produzione** (es. Branch MAIN/DEFAULT)
- I **Security Gate *POSSONO*** essere **impostati** su **qualunque percorso**, ma **DEVONO** essere **presenti e attivi** sul percorso per il **rilascio** in **produzione**
- **Definizione**, **monitoraggio** ed **enforcing** di **linee guida** e **regole aziendali**

Aspetti da **trattare** con particolare **attenzione** ed **effort**

La Pratica

… ma più complesso realizzare Security Check-out

SecDevOps



▶ **Obiettivo**: essere **certi** che ciò che arriva in **produzione** abbia superato **TUTTI** i **controlli di sicurezza** mediante la realizzazione di un **Security Checkout**

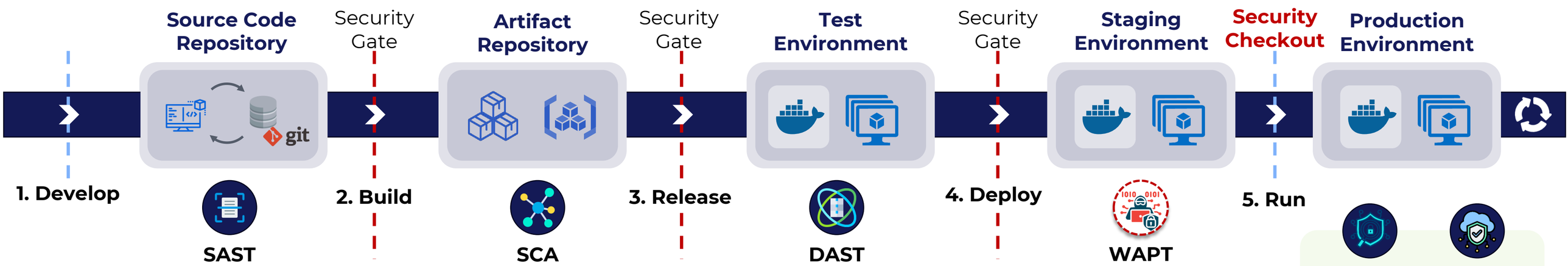
Per sviluppare il **Security Checkout** è necessario **centralizzare e registrare**:

- **Identificativi** di tutti i **componenti sw** (version, build e release ID)
- **Esito** e **timestamp** di tutti i **controlli effettuati**

Il **Security Checkout** verifica che **per ciascuno dei componenti sw** in fase di **rilascio in produzione** siano **superati tutti i controlli di sicurezza AST associati** ai rispettivi **identificativi**

La Teoria
...e poi shift right

SecDevOps



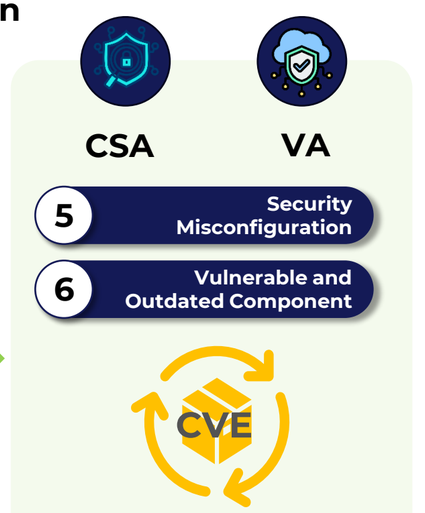
Superato il **Security Checkout**, quali **problemi** di sicurezza si possono manifestare a **runtime**?

- **Nuove vulnerabilità** di librerie e prodotti
- **Misconfigurazioni** introdotte in esercizio

Controlli periodici da attivare a **runtime**:

- **Vulnerability Assessment** sui server
- **Container Security Analysis** sui microservizi

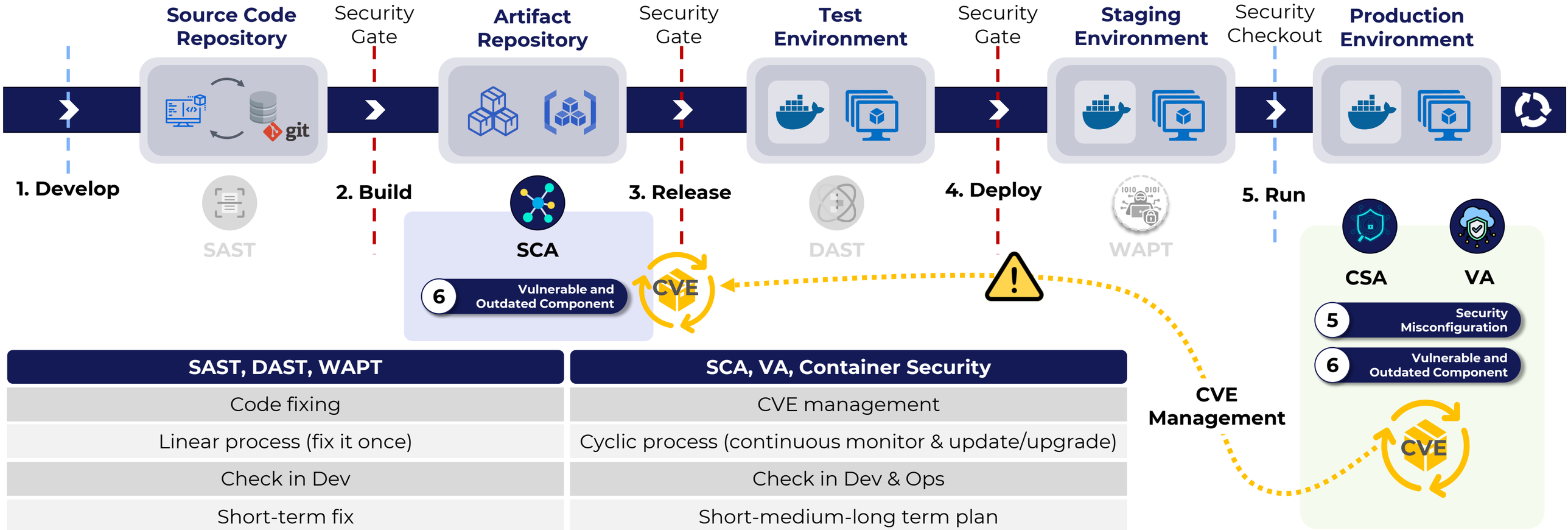
Presenza di CVE e configurazioni vulnerabili nei sistemi, nelle librerie e nei prodotti utilizzati.



Aspetti da **trattare** con particolare **attenzione** ed **effort**

La Pratica
...e poi shift back

SecDevOps



SAST, DAST, WAPT	SCA, VA, Container Security
Code fixing	CVE management
Linear process (fix it once)	Cyclic process (continuous monitor & update/upgrade)
Check in Dev	Check in Dev & Ops
Short-term fix	Short-medium-long term plan

Conclusioni

… spostarsi sulle persone

Migliorare il livello di sicurezza del codice non richiede solo un **intervento tecnologico** puntuale per inserire controlli automatici AST nel SDLC,
ma anche un **processo organizzativo** per coinvolgere le **persone** necessarie,
da affrontarsi applicando **strategie di Change Management**
soprattutto in grandi realtà:

- ✓ Chiarezza di obiettivi, di compiti e di vantaggi per chi partecipa,
- ✓ Effort essenziale e percorso graduale,
- ✓ Comunicazione bidirezionale/collaboration,
- ✓ Community & Champions,
- ✓ "Empatia" e supporto continuo,
- ✓ Commitment aziendale

Q&A

Grazie per l’attenzione!