結合 IaC 與 PaC 提供企業上雲與應用部署（K8S）的資安偵測與修補

Wistron DX lab
緯創數位轉型技術實驗室
Institute of Advanced Technology and Research for Digital Transformation

April, 2022

一位任職於緯創的IT 職人

Taiwan Data Engineering Association
台灣資料工程協會
SINCE 2017

緯創IT先進技術實驗室 witlab

DataCon.TW 2018
第十屆臺灣Hadoop 使用者社群年會
暨
第二屆臺灣資料工程年會

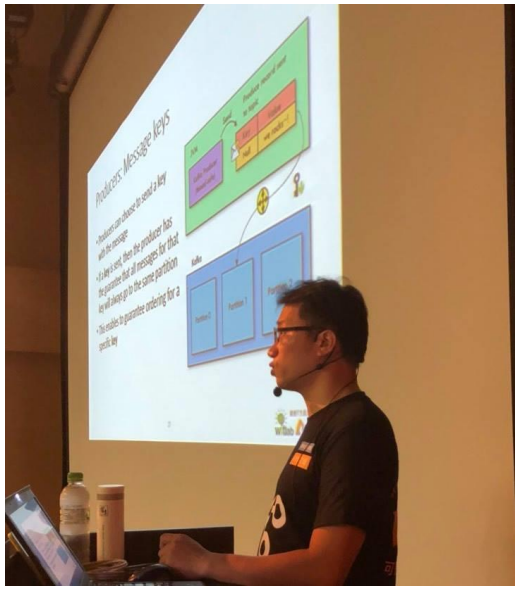
Wistron DX lab
緯創數位轉型技術實驗室
Institute of Advanced Technology and Research for Digital Transformation

ErhWen Kuo
erhwenkuo

Follow

緯創資通(Wistron)員工。在緯創創立「緯創IT先進技術實驗室(witlab)」、並於緯創協助導入Elasticsearch、MQTT、Apache Spark、Apache Flink、Apache Kafka、Keras與Tensorflow..等等在生產流程的應用及整合。

https://github.com/erhwenkuo

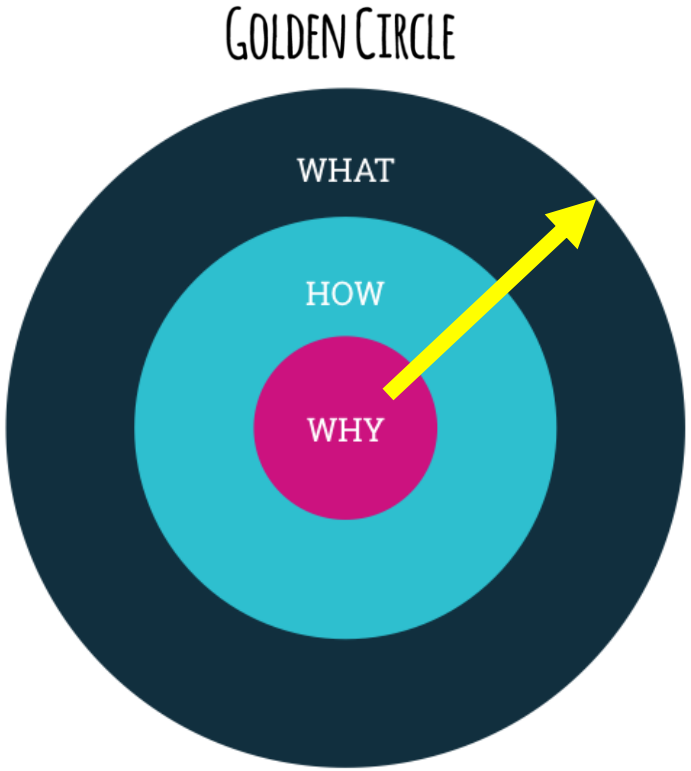


DataCon.TW 2017
9th Hadoop.TW annual conference

Real-time analytics with Flink and Druid

DataCon.TW 2018
10th Hadoop.TW / 2nd TDEA Annual Conference

Kafka "恰好一次（Exactly-once）"的資料送達保證



WHY

企業將應用系統搬遷上雲並且利用雲原生的技術與 K8S 來建構新一代的雲原生應用的情境愈來愈多。

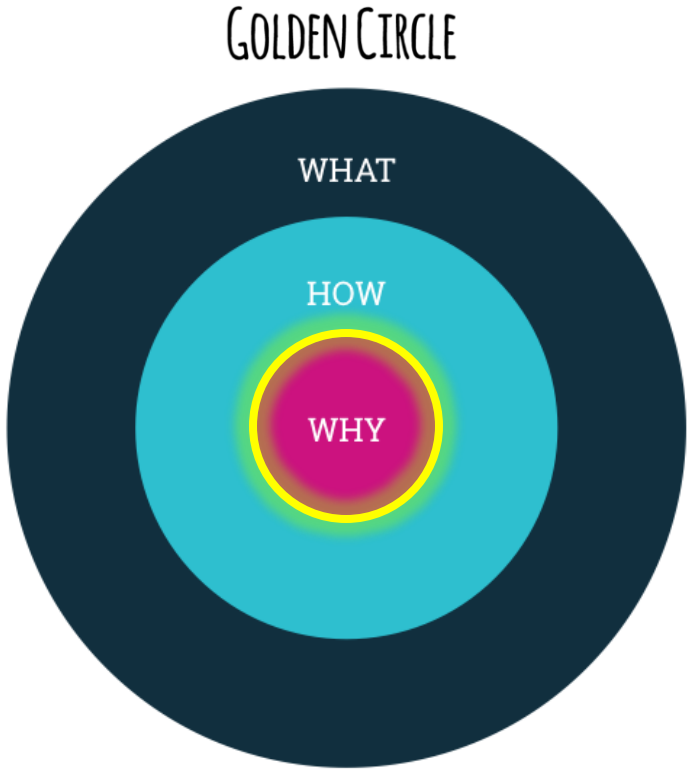
企業面臨著如何在快速迭代開發的過程, 也能夠確保資安的保證與相關的設定可以符合資安規範的挑戰。

HOW

使用 CNCF 的 OPA、Terrascan 來作為 PaC 的實作並且結合了 Terraform 的 IaC 及 Gitlab 的 Repo 來完成「測試左移」（Security Shift-left）的架構

WHAT

架構展示與說明



WHY

企業將應用系統搬遷上雲並且利用雲原生的技術與 K8S 來建構新一代的雲原生應用的情境愈來愈多。

企業面臨著如何在快速迭代開發的過程, 也能夠確保資安的保證與相關的設定可以符合資安規範的挑戰。

HOW

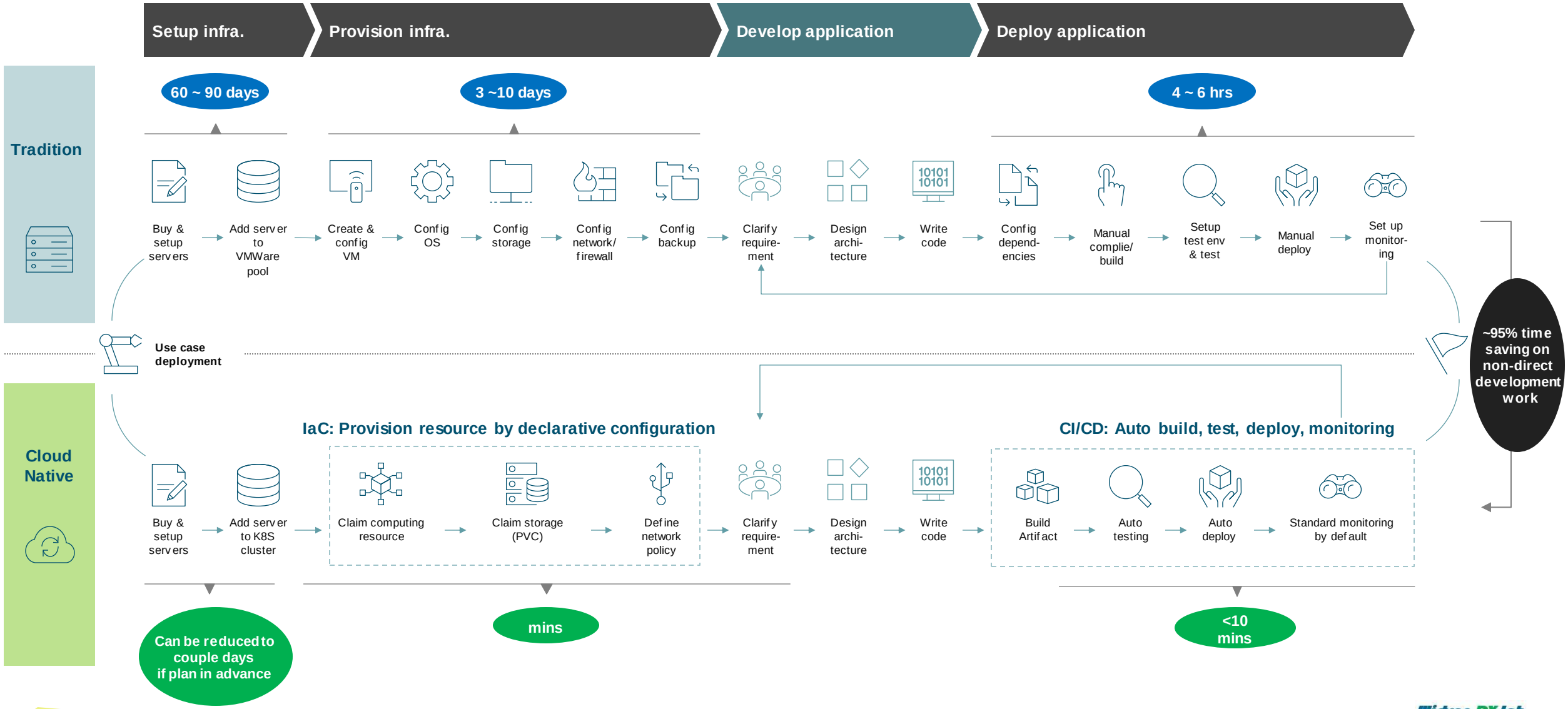
使用 CNCF 的 OPA、Terrascan 來作為 PaC 的實作並且結合了 Terraform 的 IaC 及 Gitlab 的 Repo 來完成「測試左移」（Security Shift-left）的架構

WHAT

架構展示與說明

WHY: 基礎架構即代碼 IaC

讓企業將基礎架構的配置方式自動化以便有效率地擴充雲端，節省時間與成本並加速應用服務的迭代與上線。



WHY: 安全策略即代碼 PaC

確保企業內的應用服務遵守合規政策 (Compliance Policy)，安全政策 (Security Policy) 跟達成最佳的維運方式。

資安趨勢部落格

最常導致資安事件的雲端組態設定錯誤

2022 年 03 月 17 日　Trend Labs 趨勢科技全球技術支援與研發中心　雲端資安, 雲端運算

組態設定錯誤看似單純且可避免，但卻是目前雲端環境最常見的一項風險。事實上，有65% 至 70% 的雲端資安挑戰都是因為組態設定錯誤而引起。

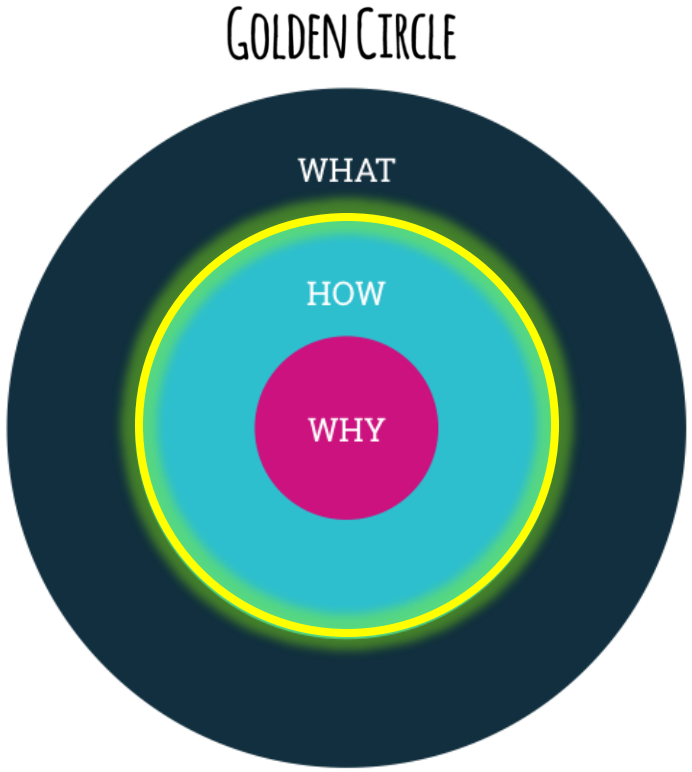
https://blog.trendmicro.com.tw/?p=71089

twcertcc
台灣電腦網路危機處理暨協調中心

資安廠商公布 SaaS 服務資安統計數字，雲端用戶資安設定高達 44% 發生錯誤

2021-08-10

https://www.twcert.org.tw/tw/cp-104-4997-d82a3-1.html



WHY

企業將應用系統搬遷上雲並且利用雲原生的技術與 K8S 來建構新一代的雲原生應用的情境愈來愈多。

企業面臨著如何在快速迭代開發的過程, 也能夠確保資安的保證與相關的設定可以符合資安規範的挑戰。

HOW

使用 CNCF 的 OPA、Terrascan 來作為 PaC 的實作並且結合了 Terraform 的 IaC 及 Gitlab 的 Repo 來完成「測試左移」（Security Shift-left）的架構

WHAT

架構展示與說明

HOW: 唯有人員、流程和技術三項徹底到位，資安才是玩真的

People Process Technology

iThome

【資安周報第64期】唯有人員、流程和技術三項徹底到位，資安才是玩真的

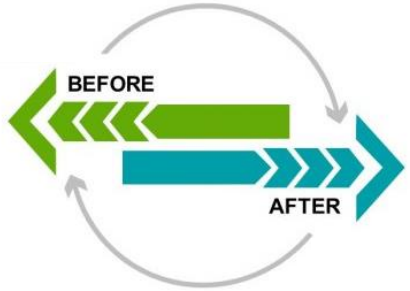
iThome電腦報舉辦「臺灣資安大會CISO論壇」，邀請本土銀行、外商銀行和高科技製造業者資訊部門主管分享如何在企業內落實資安的經驗，就算是老生常談的準則，徹底落實就是做好資安的不二法門

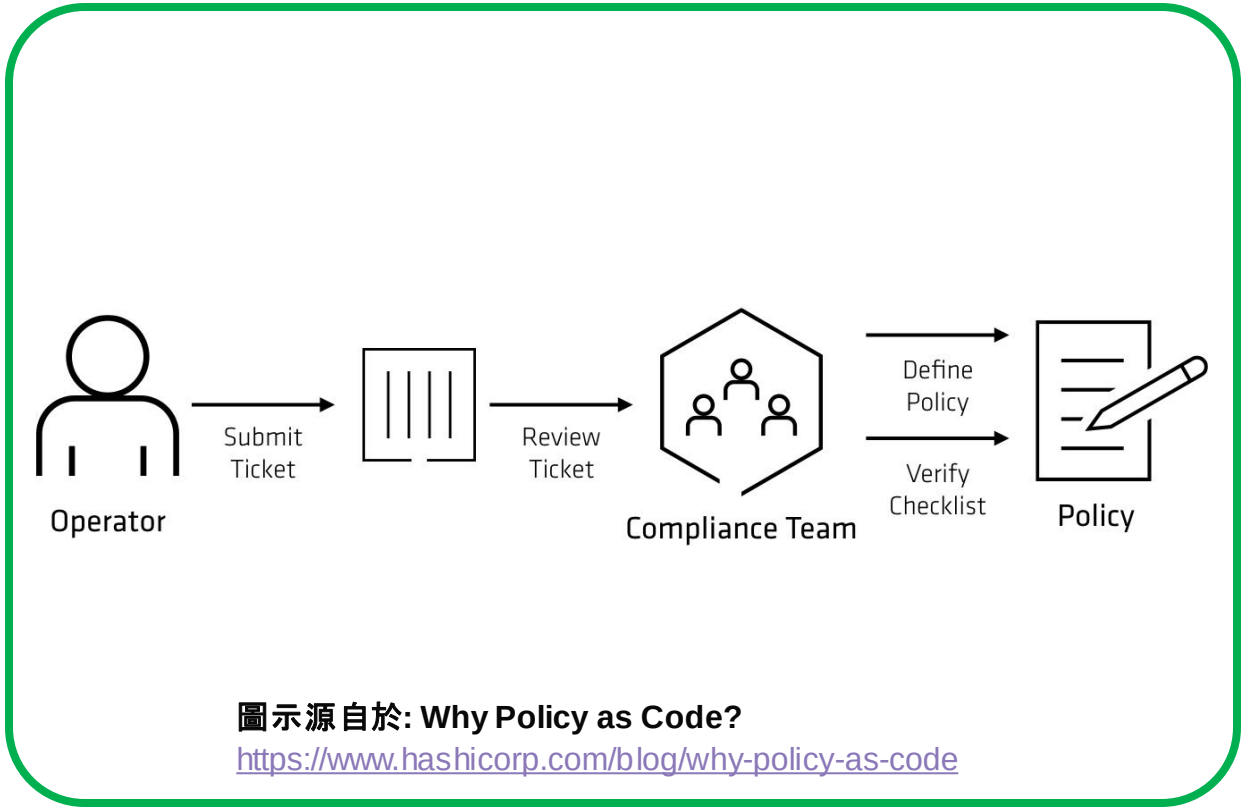
文/ 黃彥棻 | 2017-03-16 發表

https://www.ithome.com.tw/news/112813

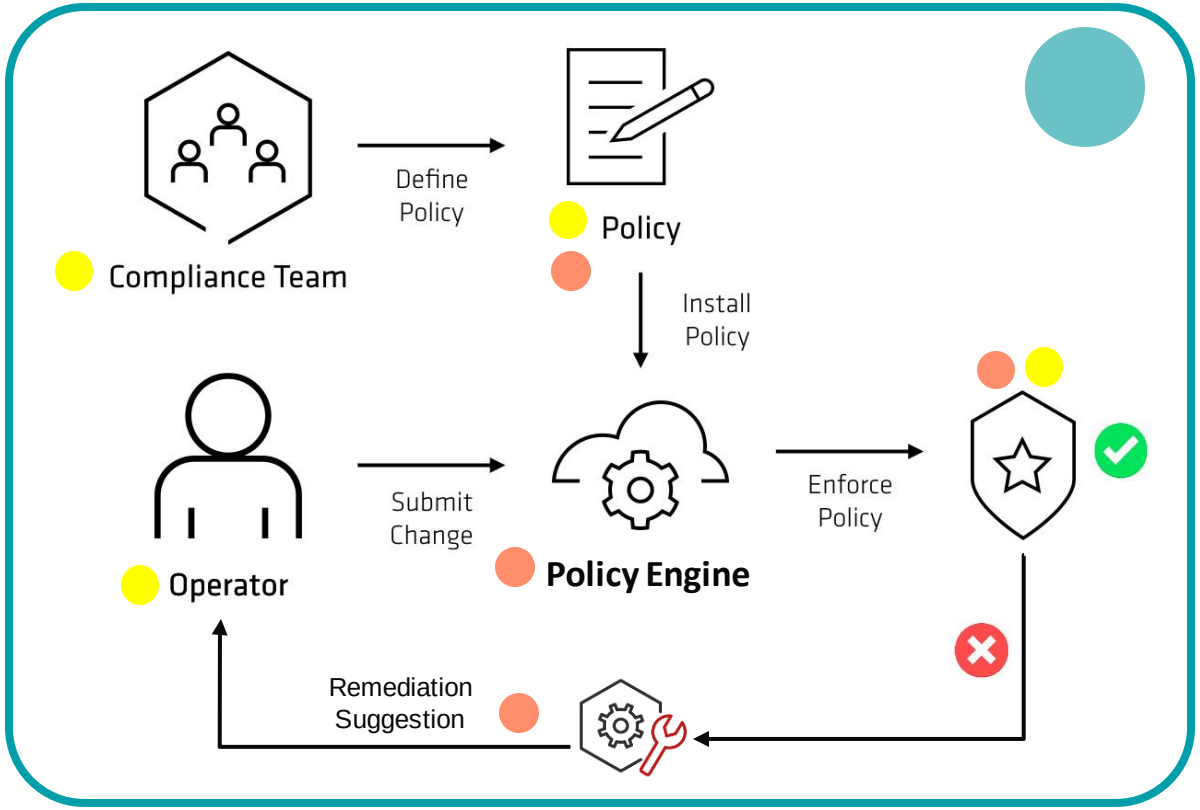
HOW: 唯有人員、流程和技術三項徹底到位，資安才是玩真的

People Process Technology



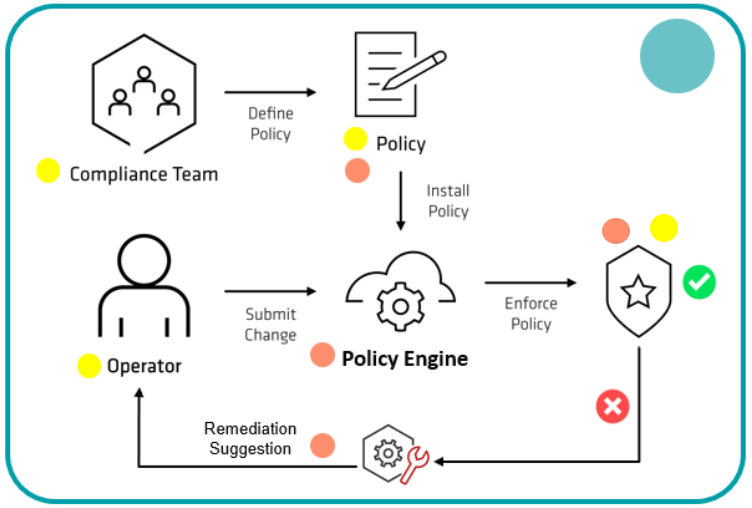


圖示源自於: Why Policy as Code?
https://www.hashicorp.com/blog/why-policy-as-code

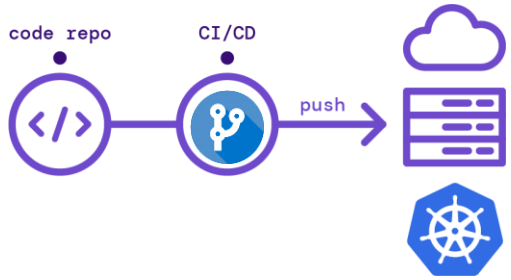


HOW: 技術實踐的關鍵設計原則

People Process Technology



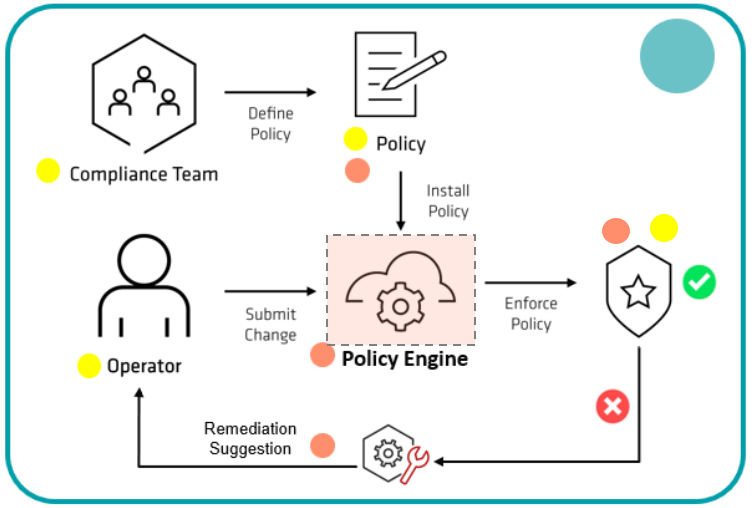
- **GitOps**
  - Git Repo 是 Single Source of Truth
  - Merge Request / Pull Request 是代碼生效與否的守門員



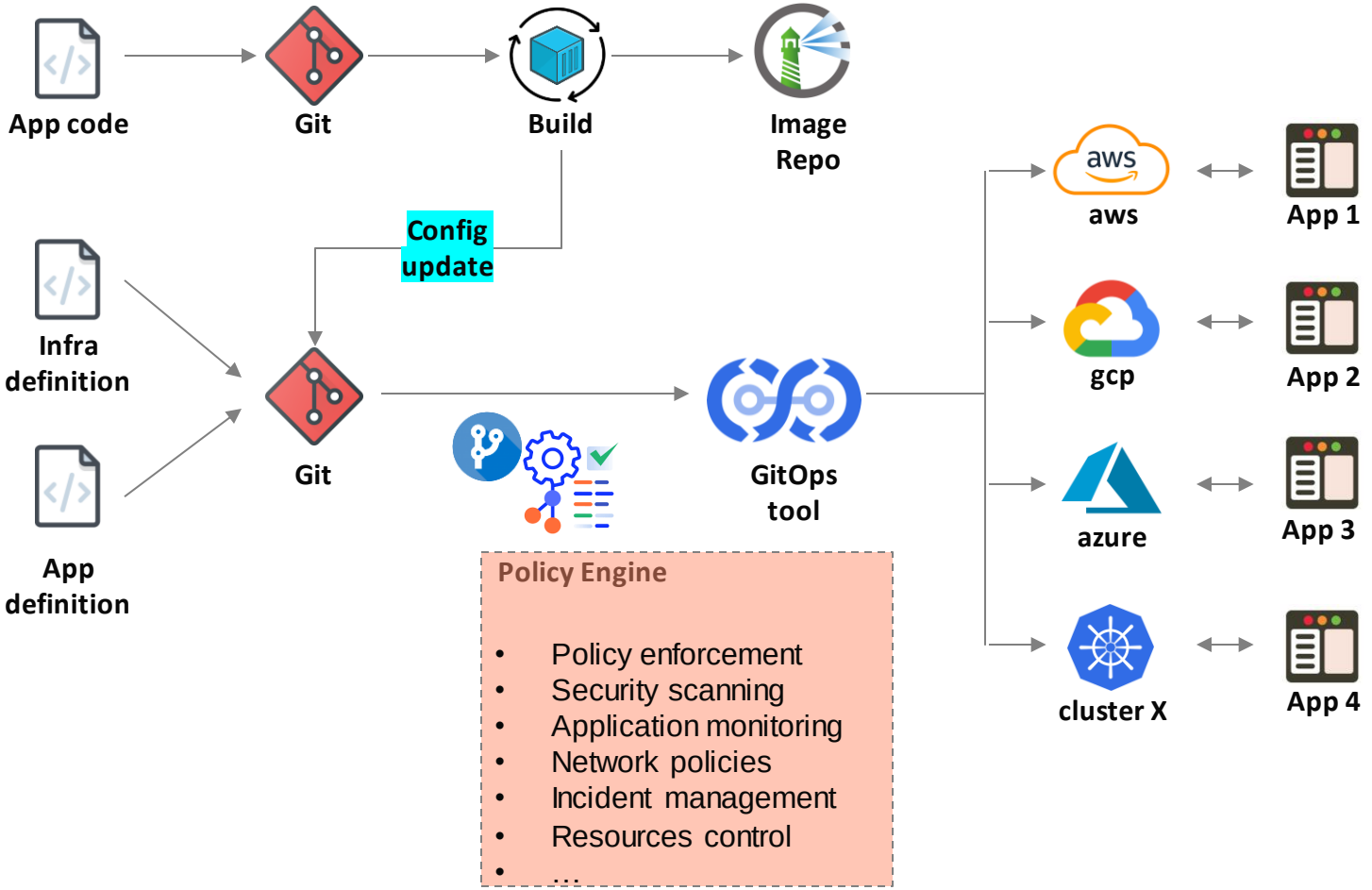
- **Security Shift-left**

HOW: 技術架構鳥瞰

People Process Technology



技術架構鳥瞰 - High level Architecture

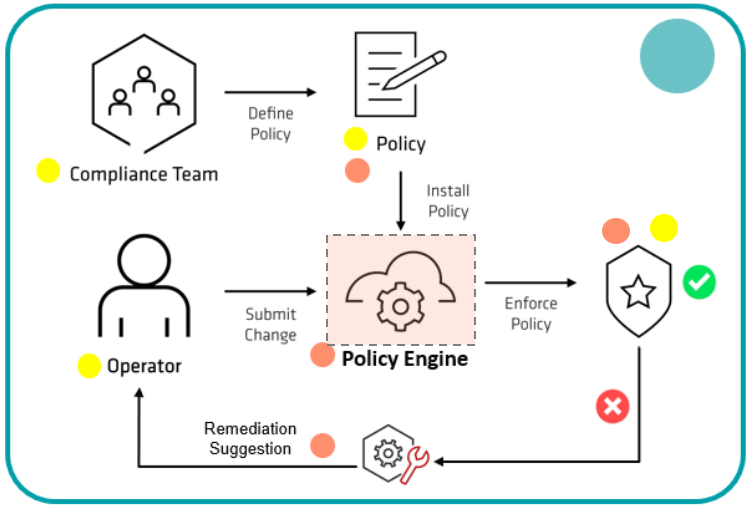


HOW: 關鍵元件選擇與比較

smalltown

MaiCoin Lead Site Reliability Engineer

People Process Technology



Nov 25, 2019

Policy as Code Introduction

https://medium.com/starbugs/policy-as-code-introduction-43332748aa4a

Oct 26, 2021

Shift Left Testing — Policy as Code 工具大比拼

https://medium.com/starbugs/shift-left-testing-policy-as-code-%E5%B7%A5%E5%85%B7%E5%A4%A7%E6%AF%94%E6%8B%BC-dcd6840a0592

checkov by bridgecrew

HashiCorp Sentinel

terrascan by accurics

Open Policy Agent

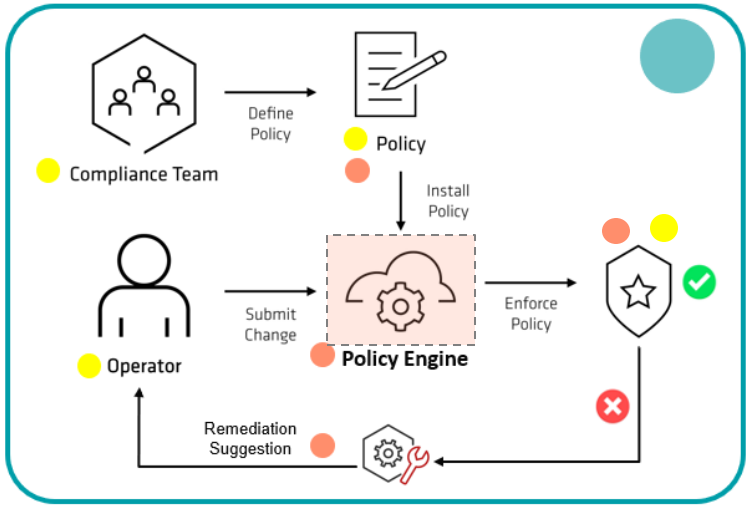
tfsec

PaC Tool	Vendor	Language	Support Platforms	Policy Language	Default Policy
checkov	Bridgecrew (Palo Alto Networks)	Python	1st	Python	1st
sentinel	HashiCorp	Go	3rd	Sentinel	4th
terrascan	Accurics (Tenable)	Go	2nd	Rego	2nd
tfsec	Aqua Security	Go	4th	JSON	3rd

HOW: Open Policy Agent (OPA) 這個通用的好東西

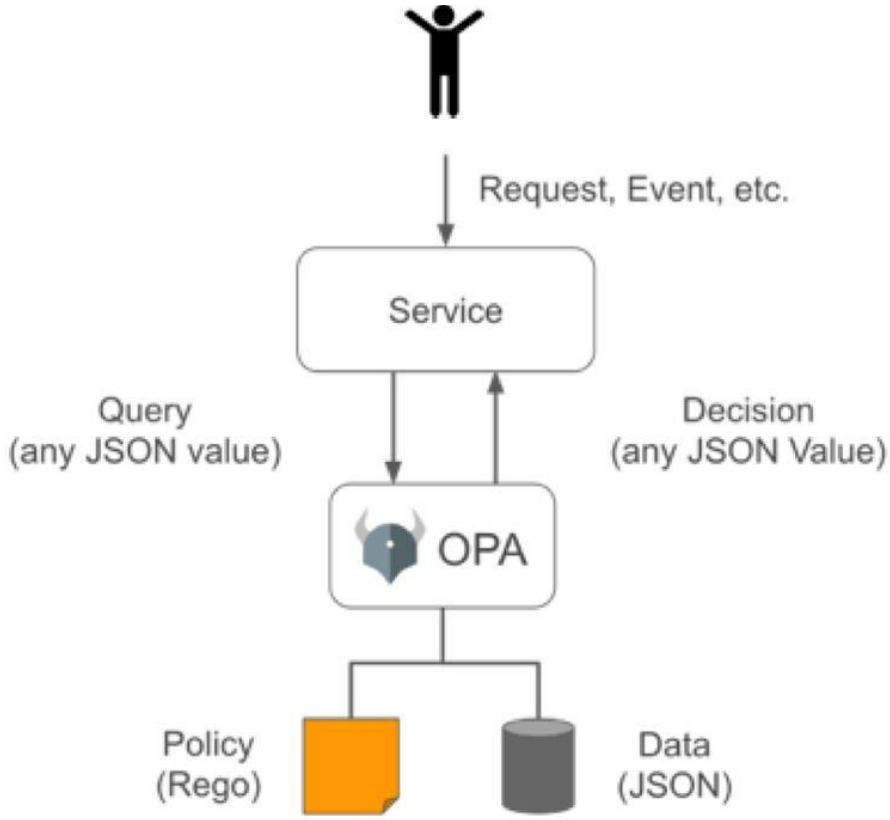
People Process Technology

OPA 是通用型訪問控制、授權和策略引擎



Open Policy Agent

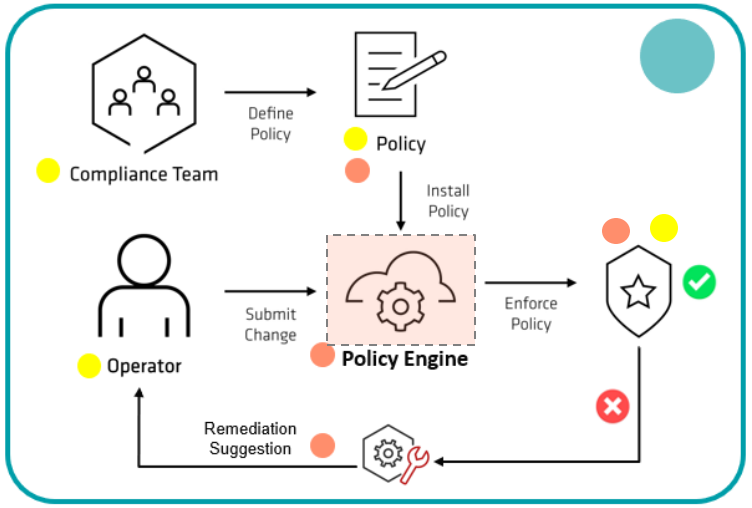
https://www.openppolicyagent.org/



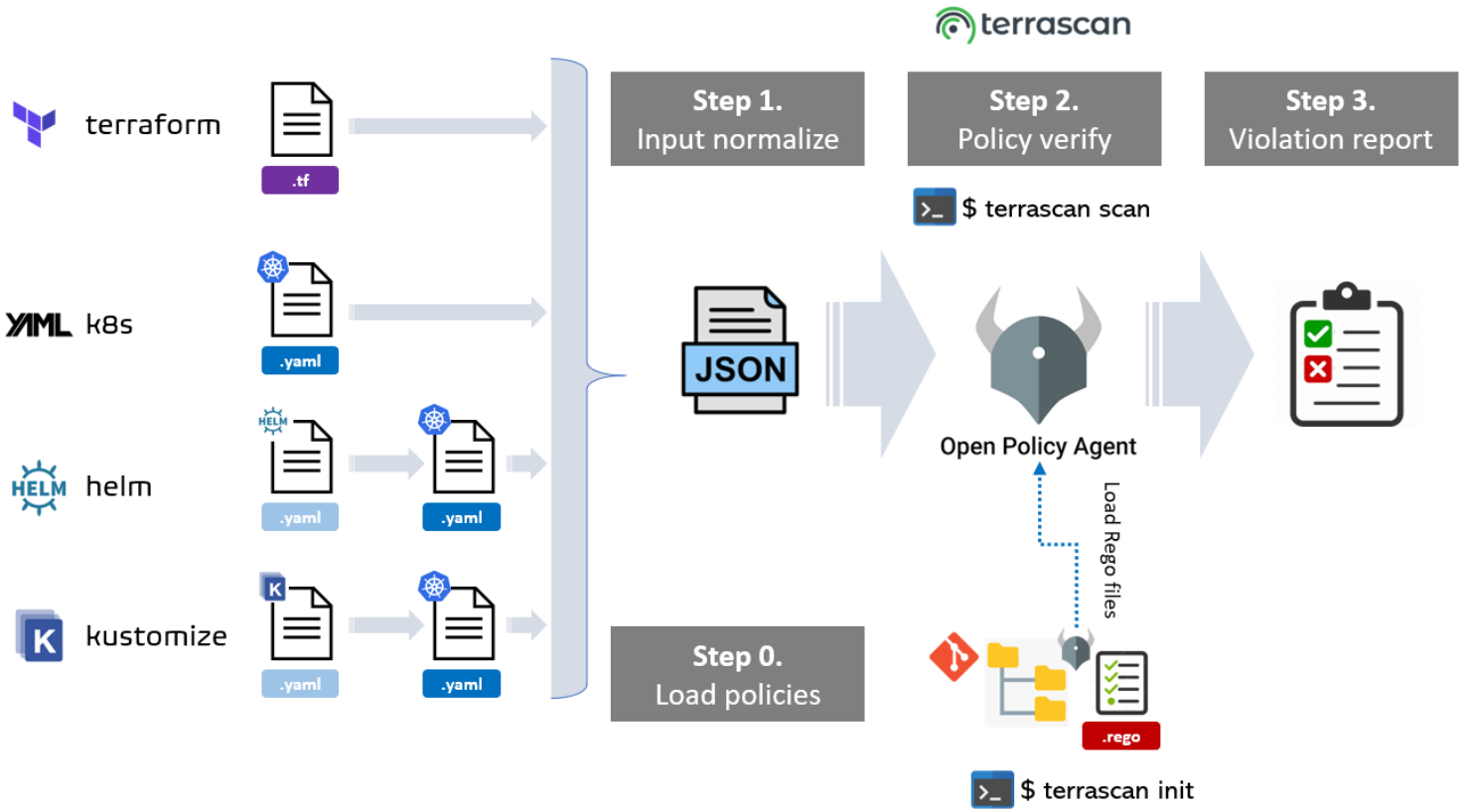
HOW: Terrascan 開源的Policy Engine

People Process Technology

OPA + Terrascan 成為一種策略引擎解決方案



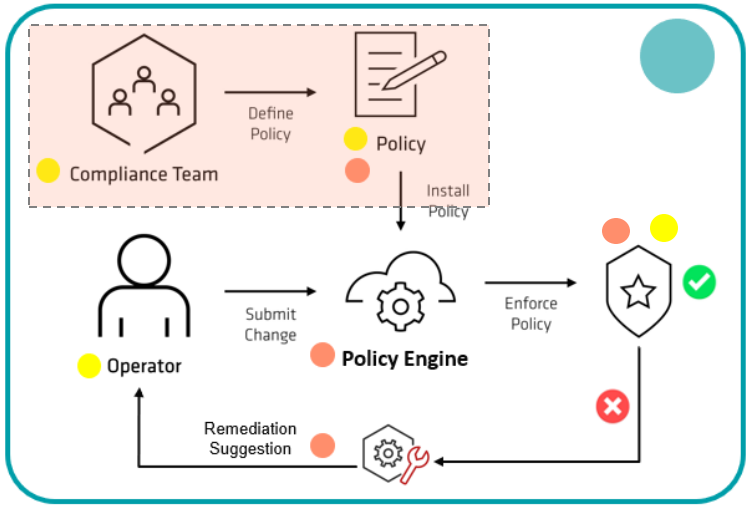
https://runterrascan.io/

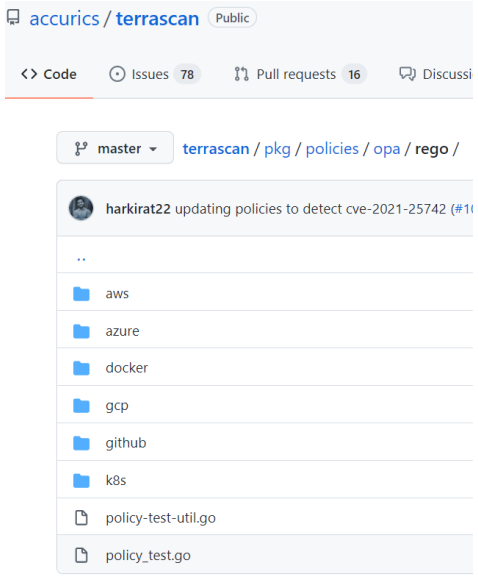


HOW: Terrascan 開源的Policy Engine

People Process Technology

Terrascan 有現成760+開箱即用的Rego策略



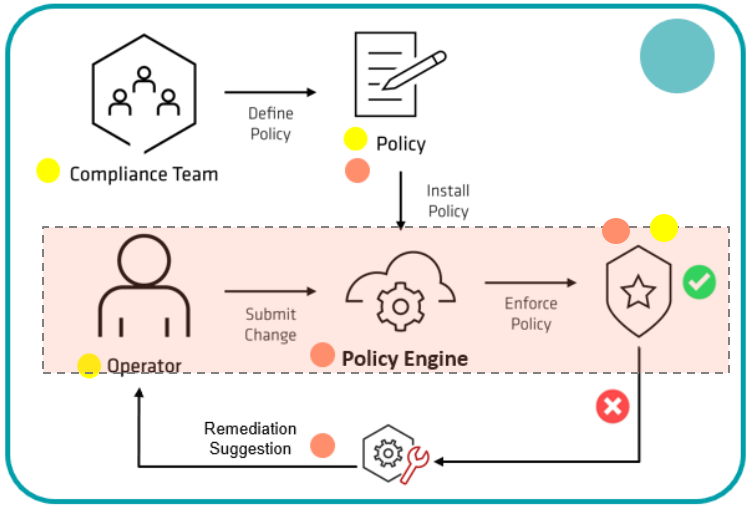


Count By - Rule ID	Column				
Row	aws	azure	gcp	k8s	Total
Compliance Validation	**15**	**4**	**10**	**2**	**31**
HIGH	6		2	1	9
LOW	3	2	8		13
MEDIUM	6	2		1	9
Configuration and Vulnerability Analysis	**1**				**1**
MEDIUM	1				1
Data Protection	**26**	**5**	**2**	**2**	**35**
HIGH	17	3			20
MEDIUM	9	2	2	2	15
Identity and Access Management	**64**	**5**	**14**	**15**	**98**
HIGH	25	3	8	3	39
LOW	36	1	3		40
MEDIUM	3	1	3	12	19
Infrastructure Security	**161**	**146**	**194**	**15**	**516**
HIGH	66	52	64	2	184
LOW	49	43	64	2	158
MEDIUM	46	51	66	11	174
Logging and Monitoring	**16**	**12**	**6**		**34**
HIGH	4	2	2		8
LOW	5		3		8
MEDIUM	7	10	1		18
Resilience	**4**	**4**	**1**		**9**
HIGH	1	1			2
MEDIUM	3	3	1		7
Security Best Practices	**16**	**2**	**7**	**9**	**34**
HIGH	2	1			3
LOW	5		7	5	17
MEDIUM	9	1		4	14
Total	**303**	**178**	**234**	**43**	**758**

HOW: Terrascan 有分類與分級的Policy

People Process Technology

開發團隊送出 Infra / App 設定的改變



Open Policy Agent + terrascan

Resource: aws_s3_bucket

Provides a S3 bucket resource.

Private Bucket w/ Tags

```
resource "aws_s3_bucket" "b" {
  bucket = "my-tf-test-bucket"
  acl    = "private"

  tags = {
    Name        = "My bucket"
    Environment = "Dev"
  }
}
```

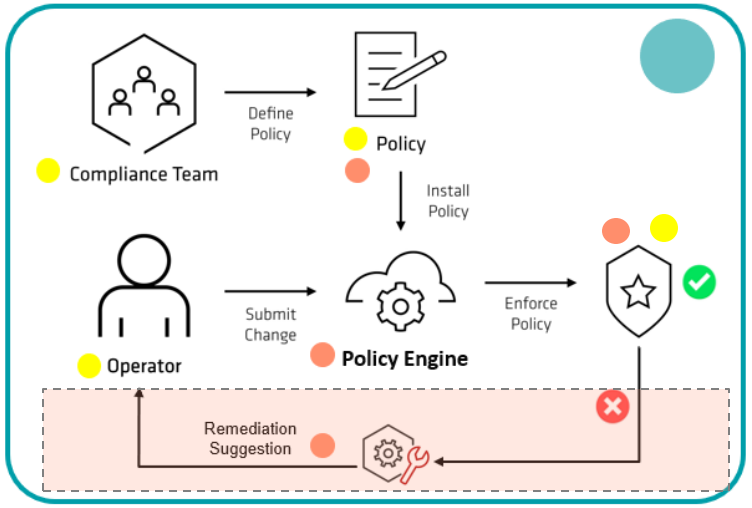
OPA Policy

```
$ terrascan scan -f private_bucket_with_tags.tf -o yaml
results:
    violations:
        - rule_name: s3BucketAccessLoggingDisabled
          description: Ensure S3 buckets have access logging enabled.
          rule_id: AC_AWS_0497
          severity: MEDIUM
          category: Logging and Monitoring
          resource_name: b1
          resource_type: aws_s3_bucket
          module_name: root
          file: private_bucket_with_tags.tf
          line: 1
        - rule_name: s3BucketSseRulesWithKmsNull
          description: Ensure that S3 Buckets have server side encryption at rest enab
          rule_id: AC_AWS_0207
          severity: HIGH
          category: Data Protection
          resource_name: b1
          resource_type: aws_s3_bucket
          module_name: root
          file: private_bucket_with_tags.tf
          line: 1
        - rule_name: s3Versioning
          description: Enabling S3 versioning will enable easy recovery from both unin
          rule_id: AC_AWS_0214
          severity: HIGH
          category: Resilience
          resource_name: b1
          resource_type: aws_s3_bucket
          module_name: root
          file: private_bucket_with_tags.tf
          line: 1
    skipped_violations: []
    scan_summary:
```

```
low: 0
medium: 1
high: 2
```

HOW: 資安偵測與修補並需一併考量才完整

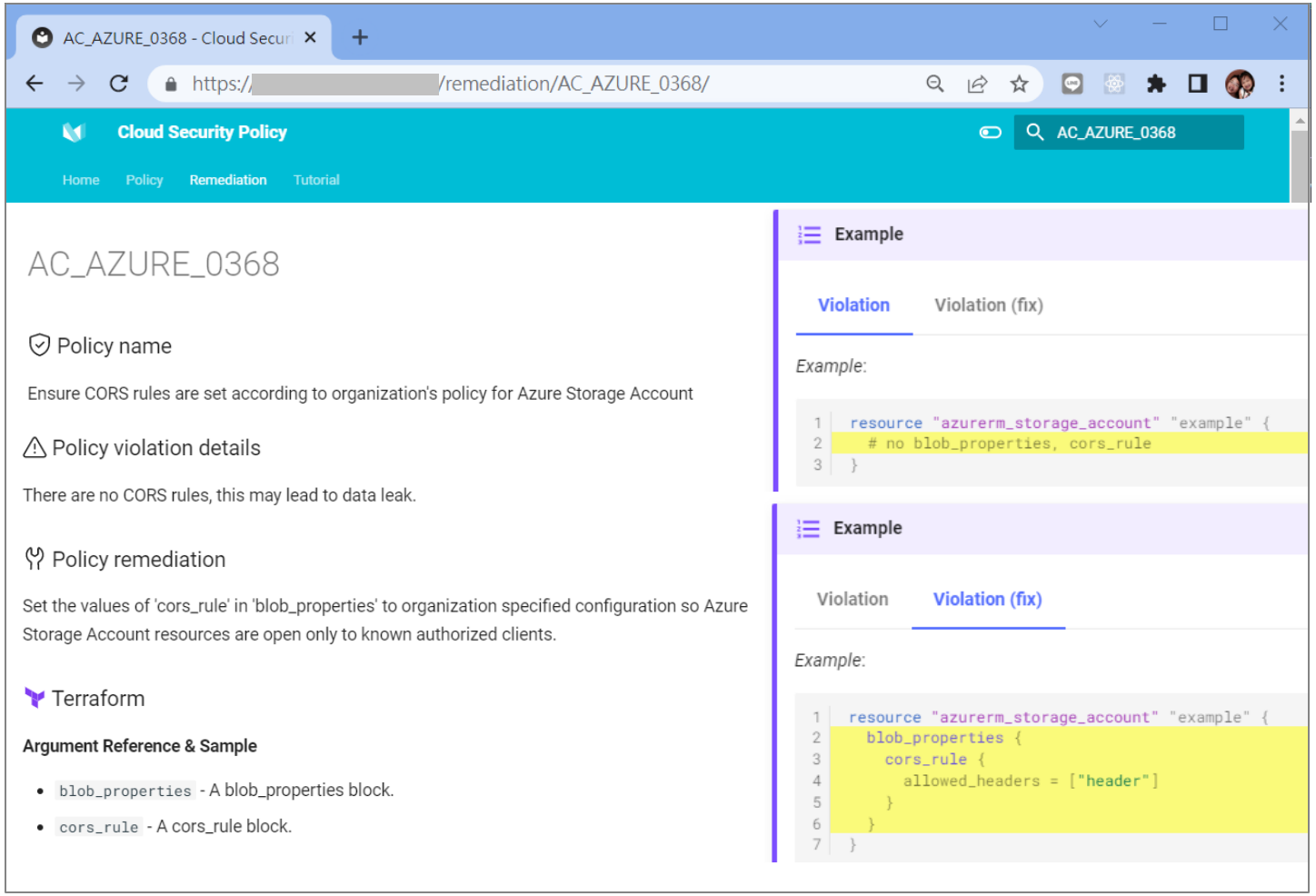
People Process Technology



Open Policy Agent + MKDOCS

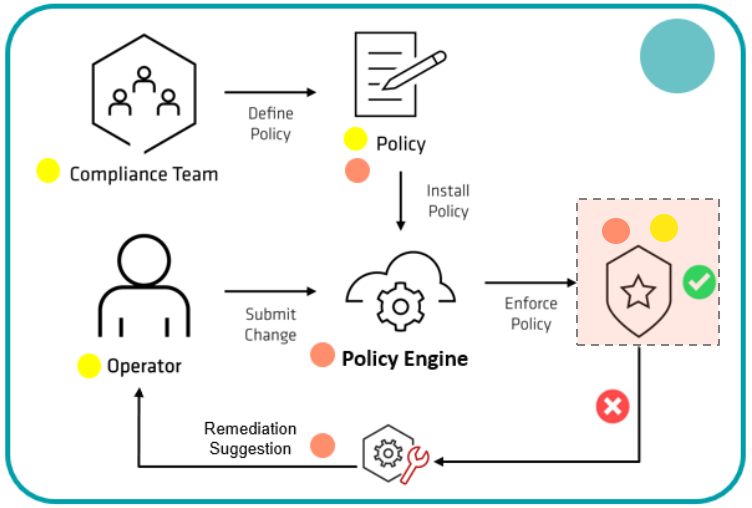
terrascan

構建 Policy Remediation 網站結予說明與建議

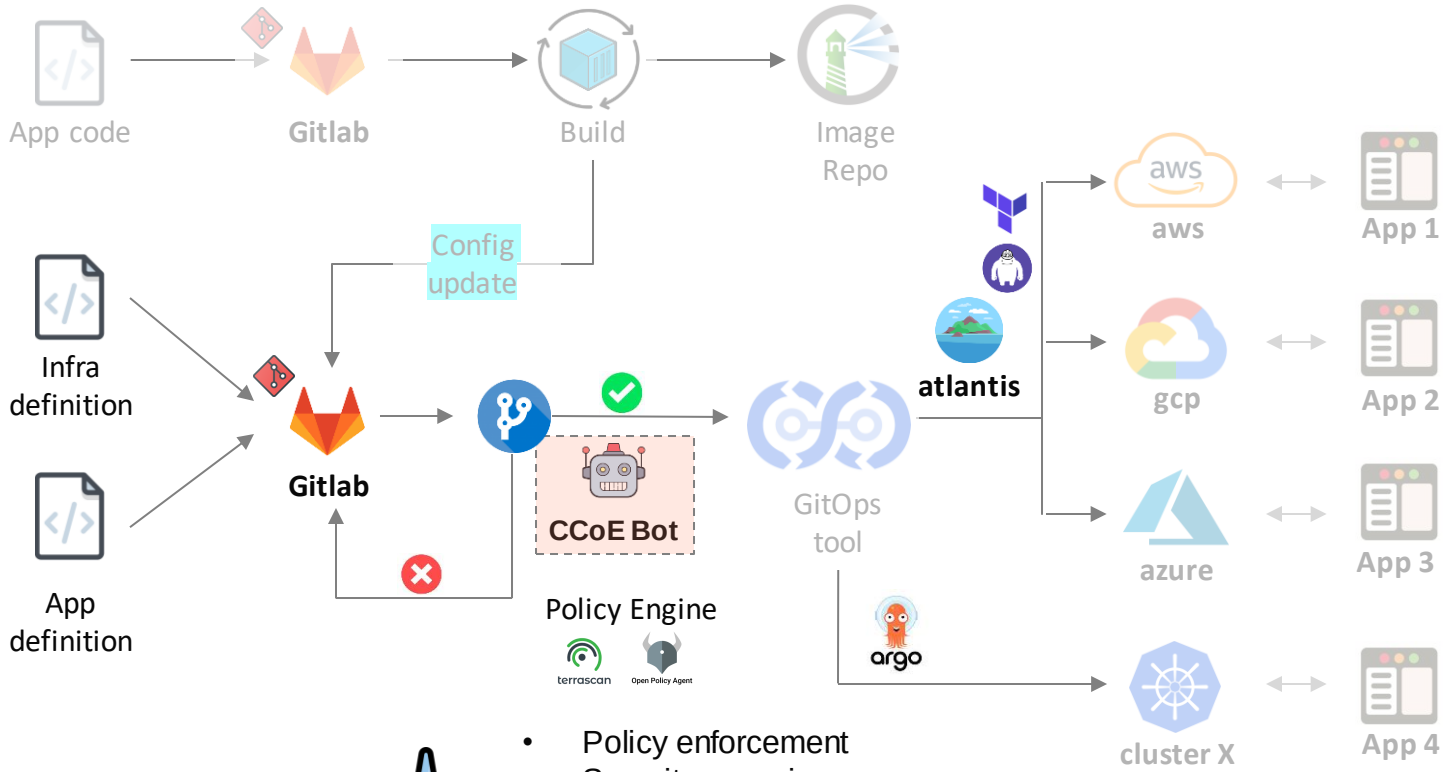


HOW: 關鍵守門員

People Process Technology



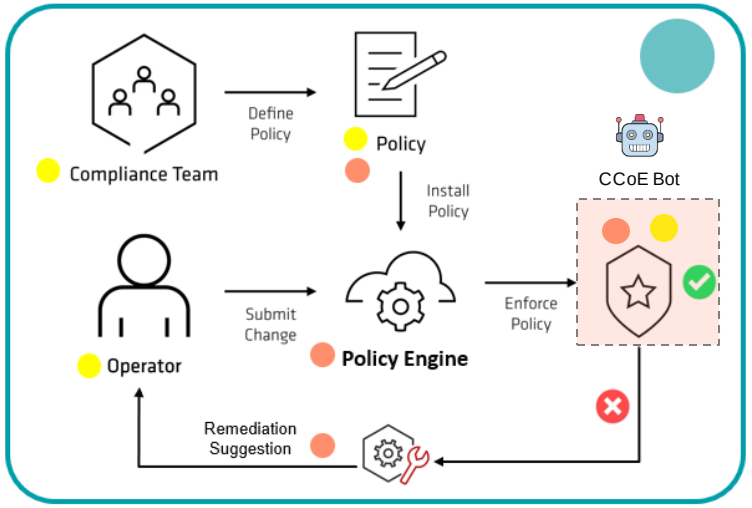
系統架構與整合



- Policy enforcement
- Security scanning
- Application monitoring
- Network policies
- Incident management
- Resources control
- …

HOW: 關鍵守門員

People Process Technology



守門員監管門戶進出/身份/代理執行關鍵動作

1 Define ownership of files from a directory

CODEOWNERS 160 Bytes

```
.gitkeep @ccoe-bot
CODEOWNER @ccoe-bot
* @ccoe-bot

project01/ @user01 @user02
project02/ @user02 @user03
project03/ @user04
project04/ @user01 @user02 @user03
```

2 Developer opens a new merge-request

Open Created just now by User04

Add new file

3 TL approves the MR

User03 @user03 · just now
ccoebot /approve

BOT CCOE @ccoe-bot · just now

Approval Summary:

- IsMergeRequestApproved: true
- ApprovalsNeeded: [@user02 @user03]
- AlreadyApprovals: [@user02 @user03 @user04 @user01]
- WaitingApprovals: []

4 TL merges the MR

User02 @user02 · 25 seconds ago
ccoebot /merge

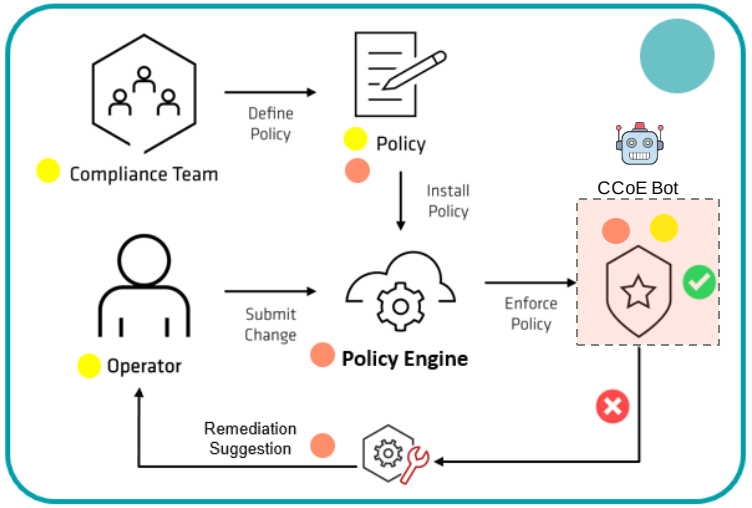
BOT CCOE @ccoe-bot merged 22 seconds ago

BOT CCOE @ccoe-bot · 22 seconds ago
The changes were merged.
※\(^o^)/※

HOW: 關鍵守門員

People Process Technology

守門員監管門戶進出/身份/代理執行關鍵動作



2 Developer opens a new merge-request

Open Created just now by User04

Add new file

3 Bot scan policy violation (via Terrascan)

BOT CCOE @ccoe-bot · 2 months ago

Policy Scan:

- k8s/podinfo/dev/

Scan Summary -

- IaC Type : all
- Policies Validated : 142
- Violated Policies : 16
- Low : 1
- Medium : 5
- High : 10

4 Operator check violation details

▼ Show scan details

```
RuleID          : AC_K8S_0064
RuleName        : securityContextUsed
Severity        : MEDIUM
ResourceType    : kubernetes_deployment
Description     : If security context is not applied t
File            : k8s\podinfo\dev\deployment.yaml
```

5 Operator use remediation suggestion to fix violation

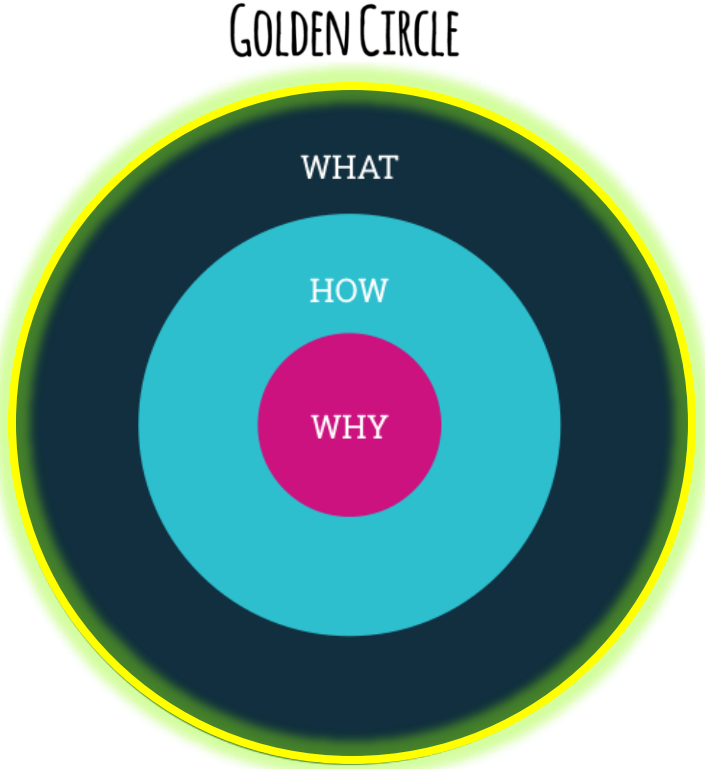
Cloud Security Policy AC_K8S_0064

Example

Violation | Violation (fix)

Example:

```
1  resource "aws_acm_certificate" "sample" {
2    domain_name       = "wistron.com"
3    validation_method = "DNS"
4  }
```



WHY

企業將應用系統搬遷上雲並且利用雲原生的技術與 K8S 來建構新一代的雲原生應用的情境愈來愈多。

企業面臨著如何在快速迭代開發的過程, 也能夠確保資安的保證與相關的設定可以符合資安規範的挑戰。

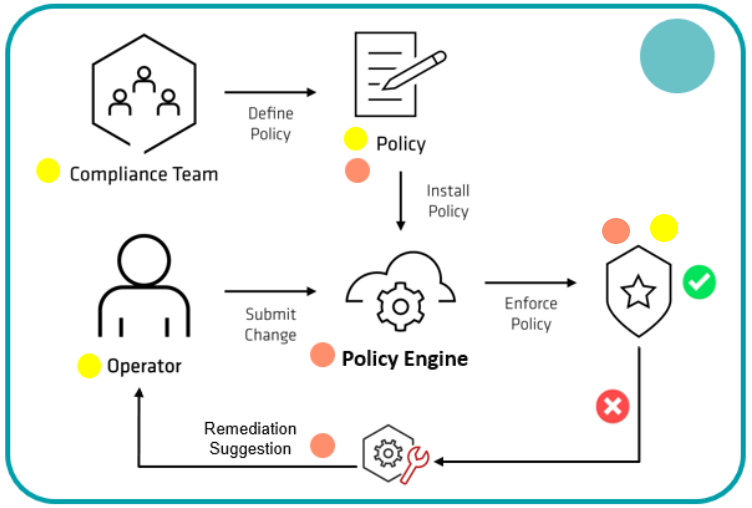
HOW

使用 CNCF 的 OPA、Terrascan 來作為 PaC 的實作並且結合了 Terraform 的 IaC 及 Gitlab 的 Repo 來完成「測試左移」（Security Shift-left）的架構

WHAT

架構展示與說明

WHAT: 架構展示與說明



系統架構與整合

People

Process gitops

Technology

Compliance Team

OPA Policy Dev Team

Product Dev Teams

Cloud Center of Excellence

Compliance Team

OPA Policy Dev Team

Gitbot / **terrascan-policy**
OPA Policy for Infosec

Gitbot / **sre-conference-demo**
iTHome SRE Conference Demo

Gitbot / **pacdocs**
Documentation for Policy as Code

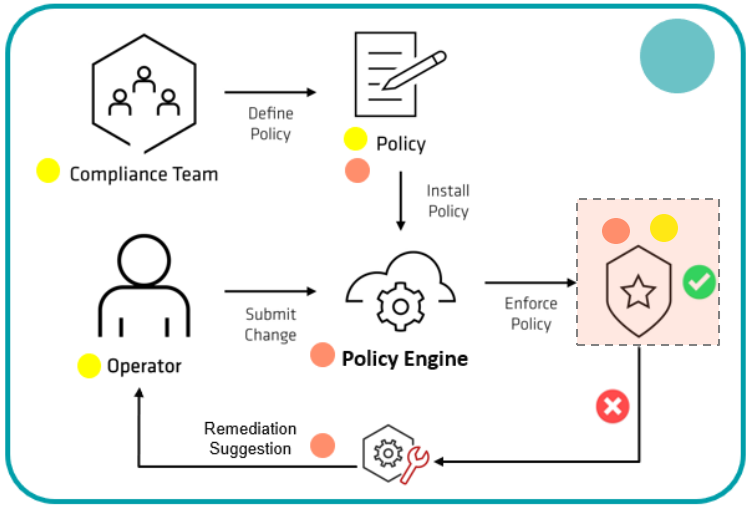
Git sync

argo

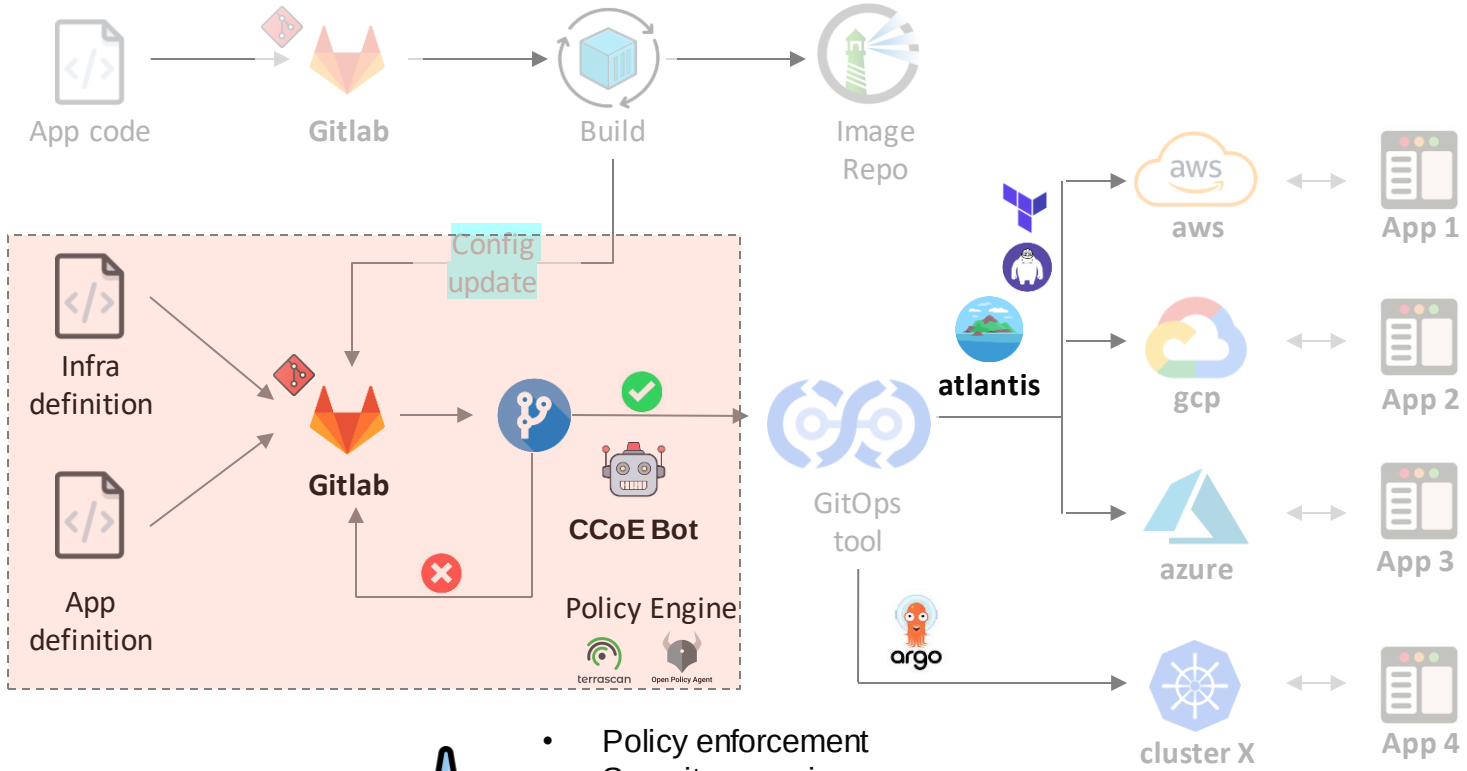
GITLAB CI/CD

WHAT: 架構展示與說明

People Process Technology



系統架構與整合



- Policy enforcement
- Security scanning
- Application monitoring
- Network policies
- Incident management
- Resources control
- …