From AI to AIOps to SRE

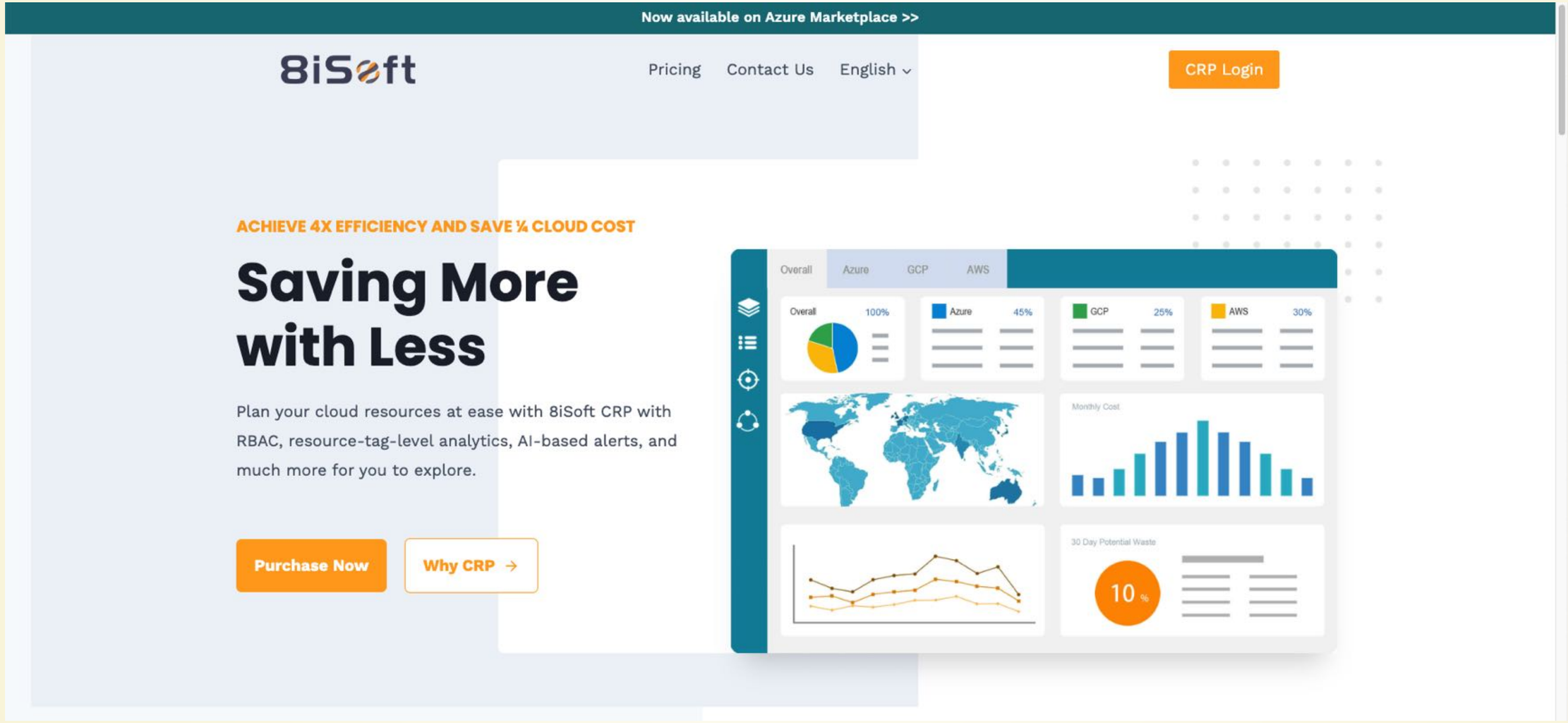
~~ SRE Conference 2023 ~~

Kuo-Chun Su


Why

Caloudi = Cloud + AI

Independent Software Vendor for Cloud Resource Planning and Cost Management



Me

蘇國鈞

- 經歷
  - 資策會數位教育研究所講師、課程經理、教學組長、未來人才中心主任
  - 卡洛地股份有限公司技術總監
- 專長
  - Parallel Processing / Parallelizing Compiler
  - Embedded System / Integrated Development Environment
  - Delphi / Visual Basic / Java / JavaScript / Scala / R / Python
  - Cloud Computing / NoSQL / Hadoop / Spark / Databricks / Synapse
  - Data Science / Machine Learning

Job Description

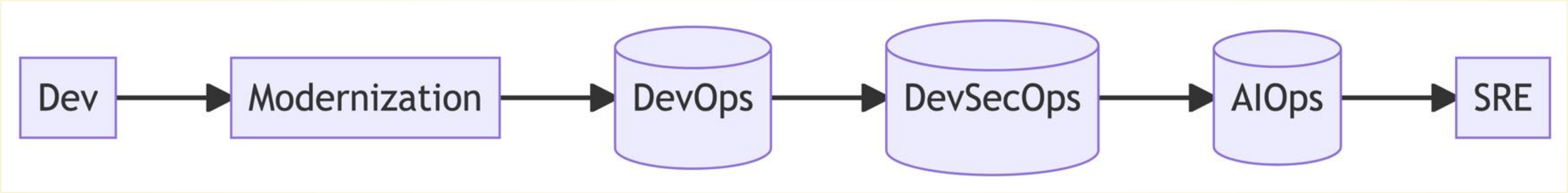
- 公司的弱電，是 CEO 買材料親自拉的。
- 公司的網路規劃跟有線網路配置，是 CEO 買材料親自佈線的。
- 公司的創意發想，是 CEO 跟 CTO 一起腦力激盪出來的。
- 公司的產品規劃跟實作，是 CTO 跟 RD Team 一起開發的。
- ...
- 在我出國休假的時候，CEO 把全公司的燈泡都換了。

在這種情況底下，身爲 Technical Director 的我，還能做些什麼？

Agenda - A Patchy SRE

我的分享主要是想介紹 SSRE - Site Security & Reliability Enhancement：

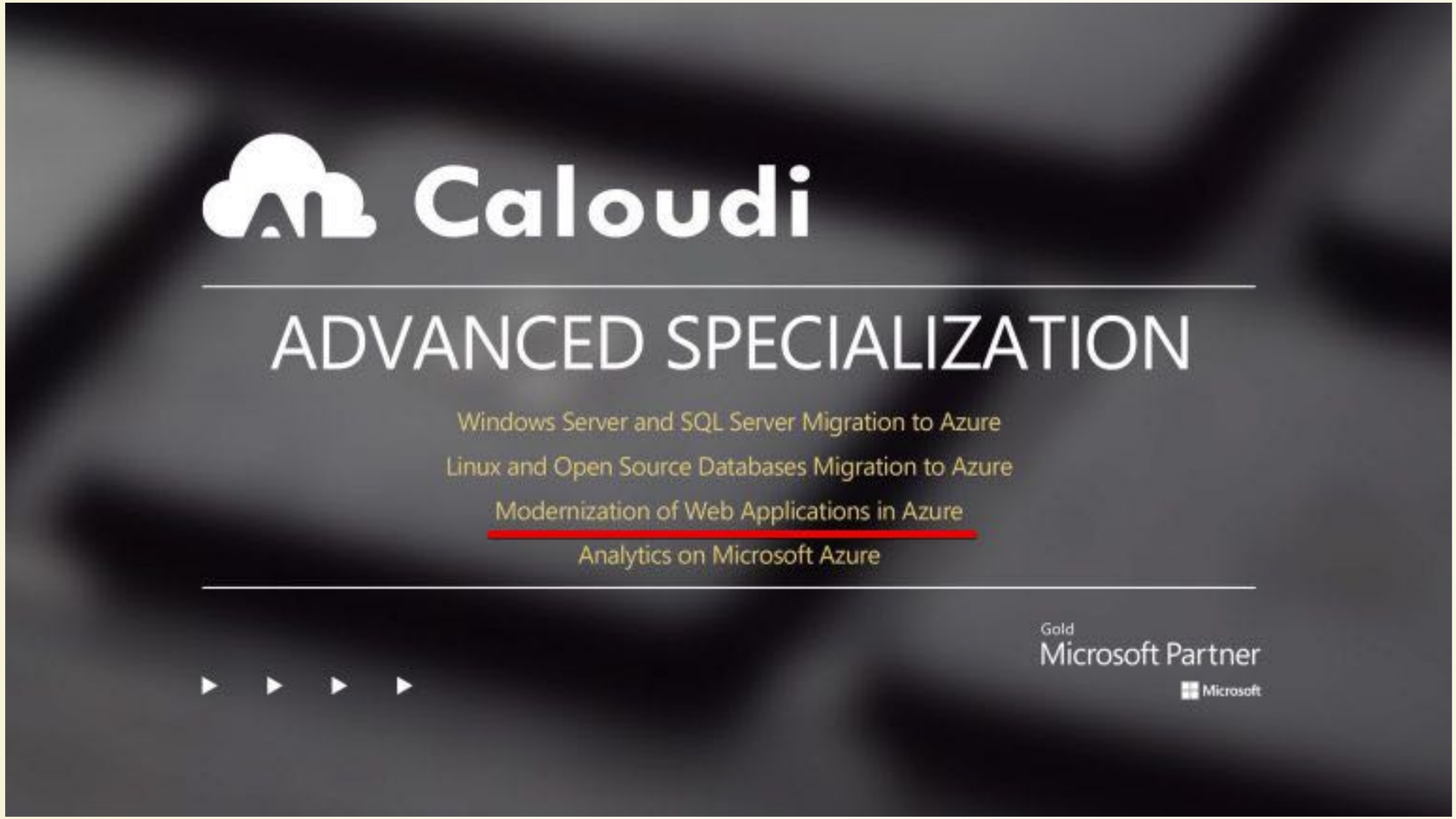
- 在公司一路成長的過程中，我們是怎麼因爲各種需求，東補西補跌跌撞撞地，就做了一些跟維運有關的事情。
- 主要就是**見招拆招** - 兵來將擋，水來土掩，路見不平，就請工人來修理。
- 雖然不是正統，不是王道，但是我相信很多企業的 SRE 團隊或多或少也有類似的經歷，這樣的鋪陳大家可能會比較有感。
- 實際上分享的重點會放在怎麼以 AIOps 幫 SRE 分憂解勞這一段。



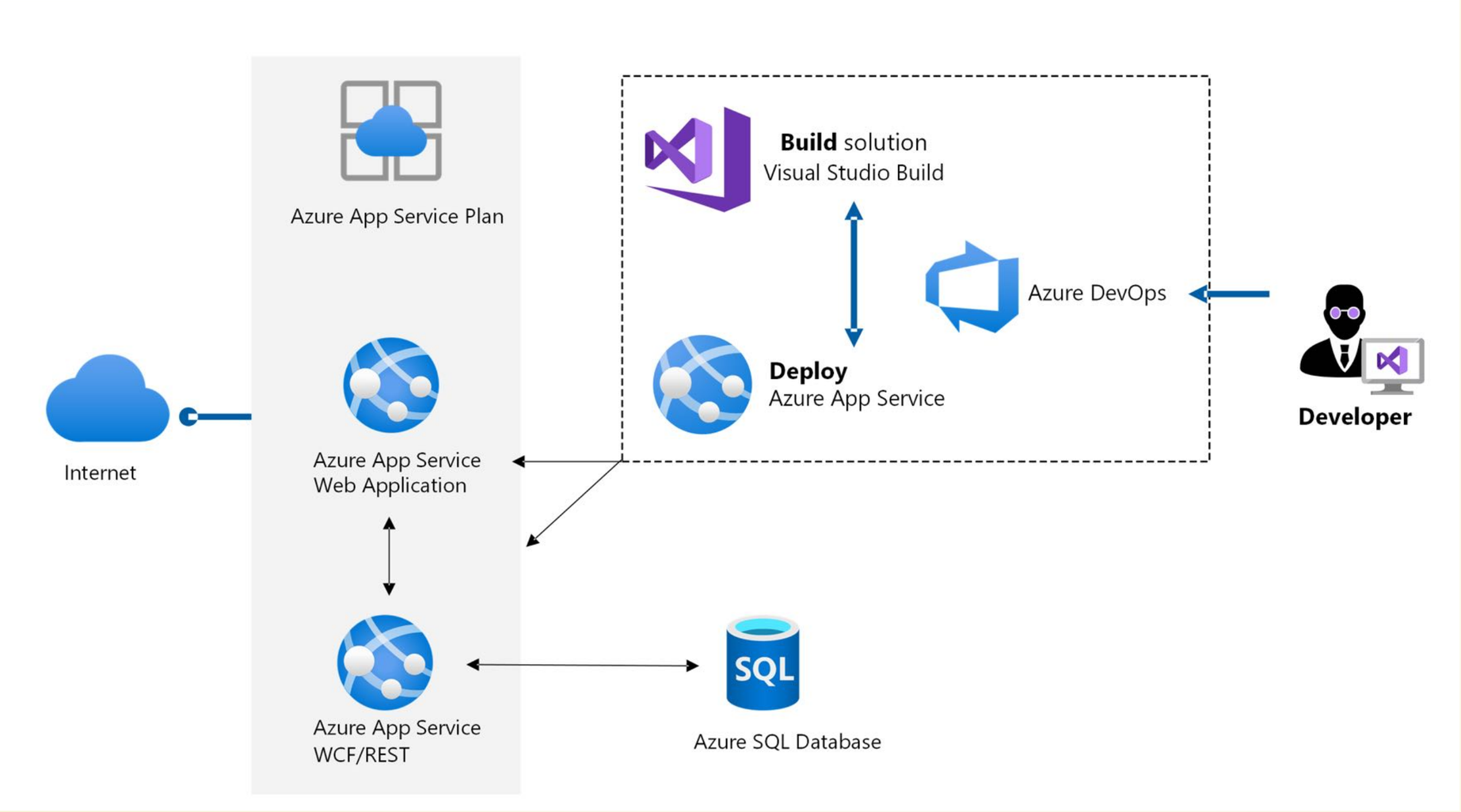
註 1.：爲了避免動搖國本，會盡量用網路上類似的圖片或是我自己畫的簡圖來取代。
註 2.：爲了取信於大家必須放的眞實圖片，會加上馬賽克之後，再放到投影片裡頭。

Trigger #1

Microsoft Cloud Partner Program

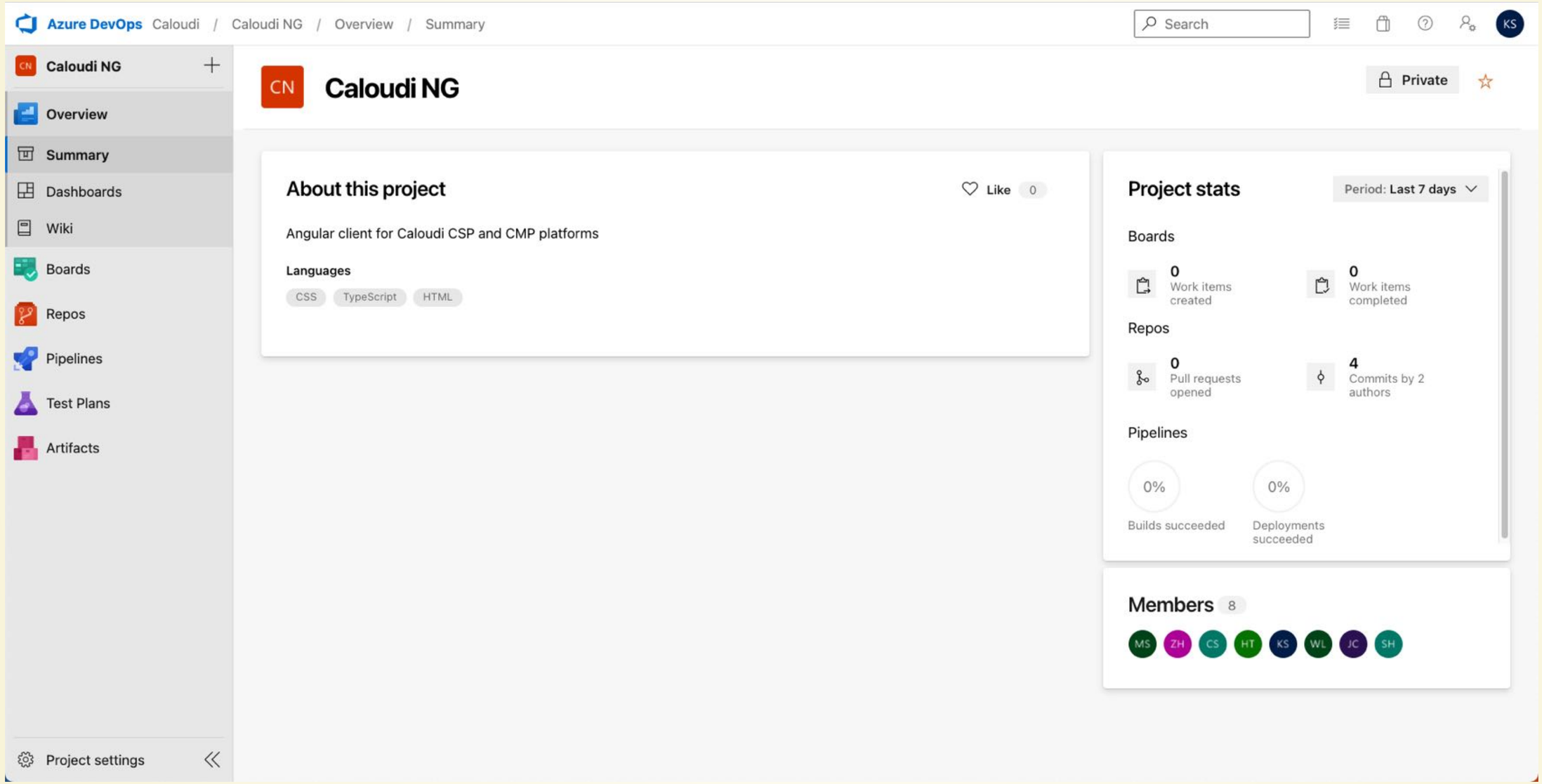


Original .NET Core Web App



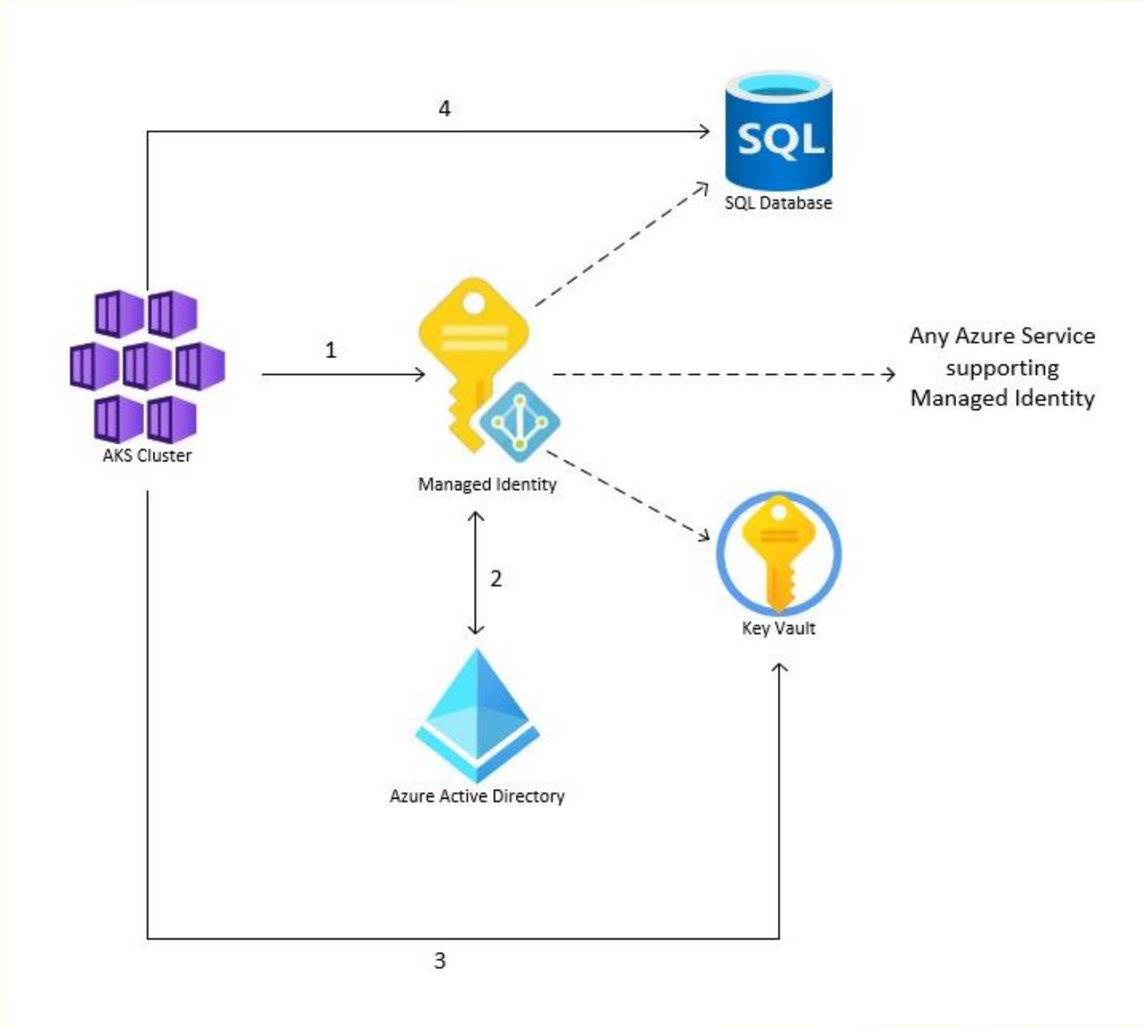
參考資料：Modernize .NET applications

Role-Based Azure DevOps Repos + CI/CD Pipelines + Boards



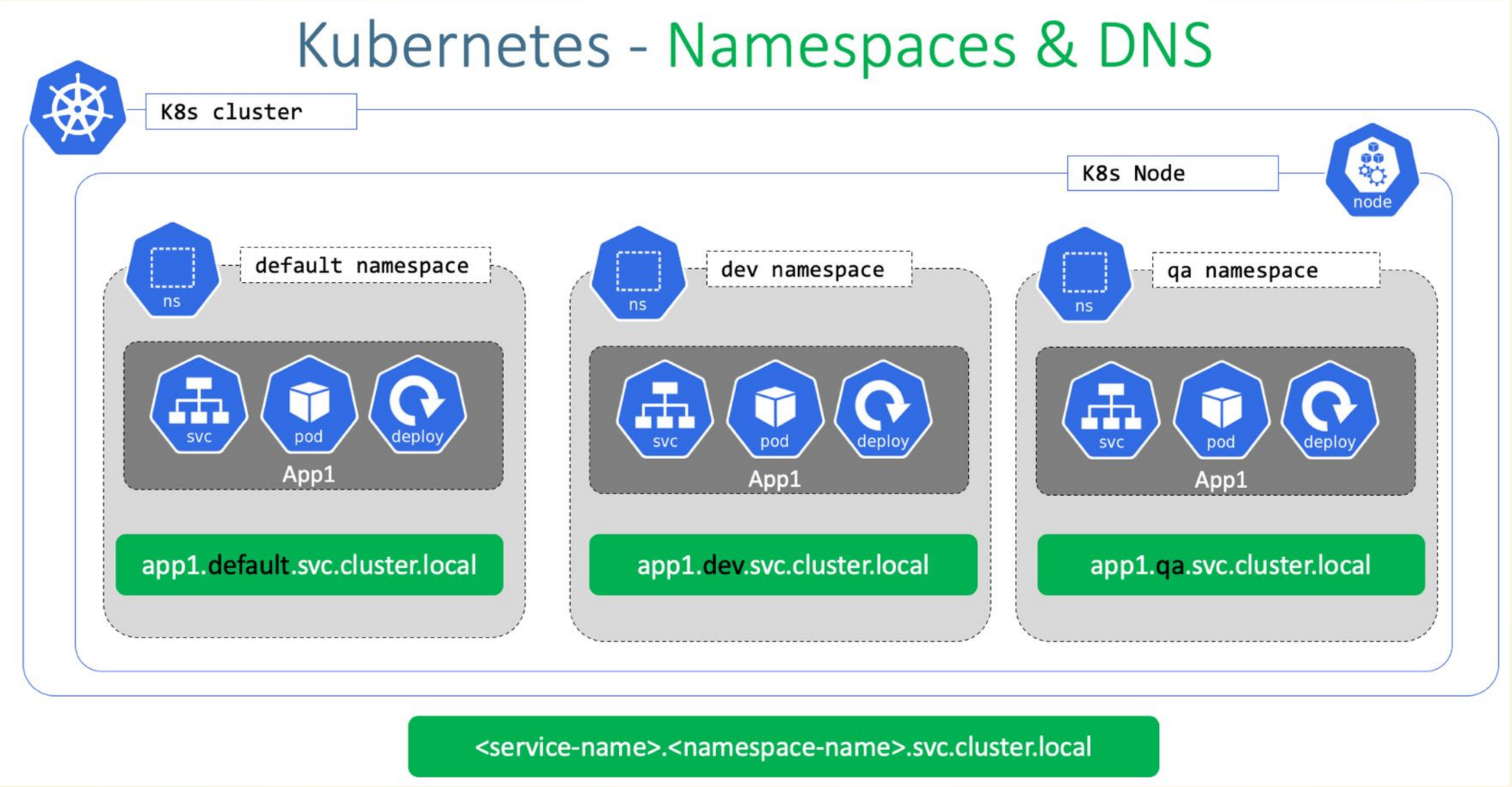
Azure Key Vault

- Security Credentials
- Connection Strings
- Configurations
- …



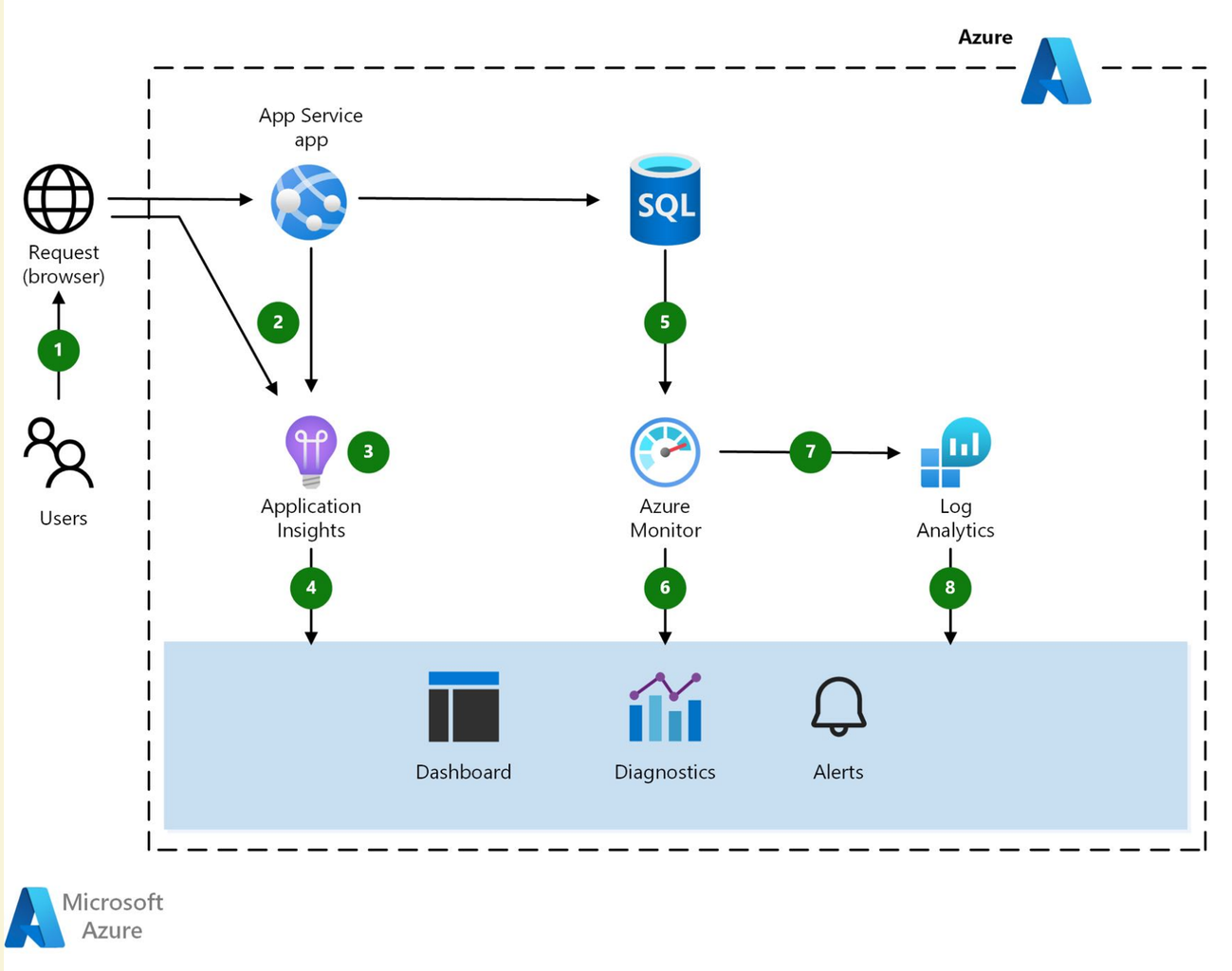
參考資料：Secure your Microservices on AKS — Part 2

Azure Kubernetes Service



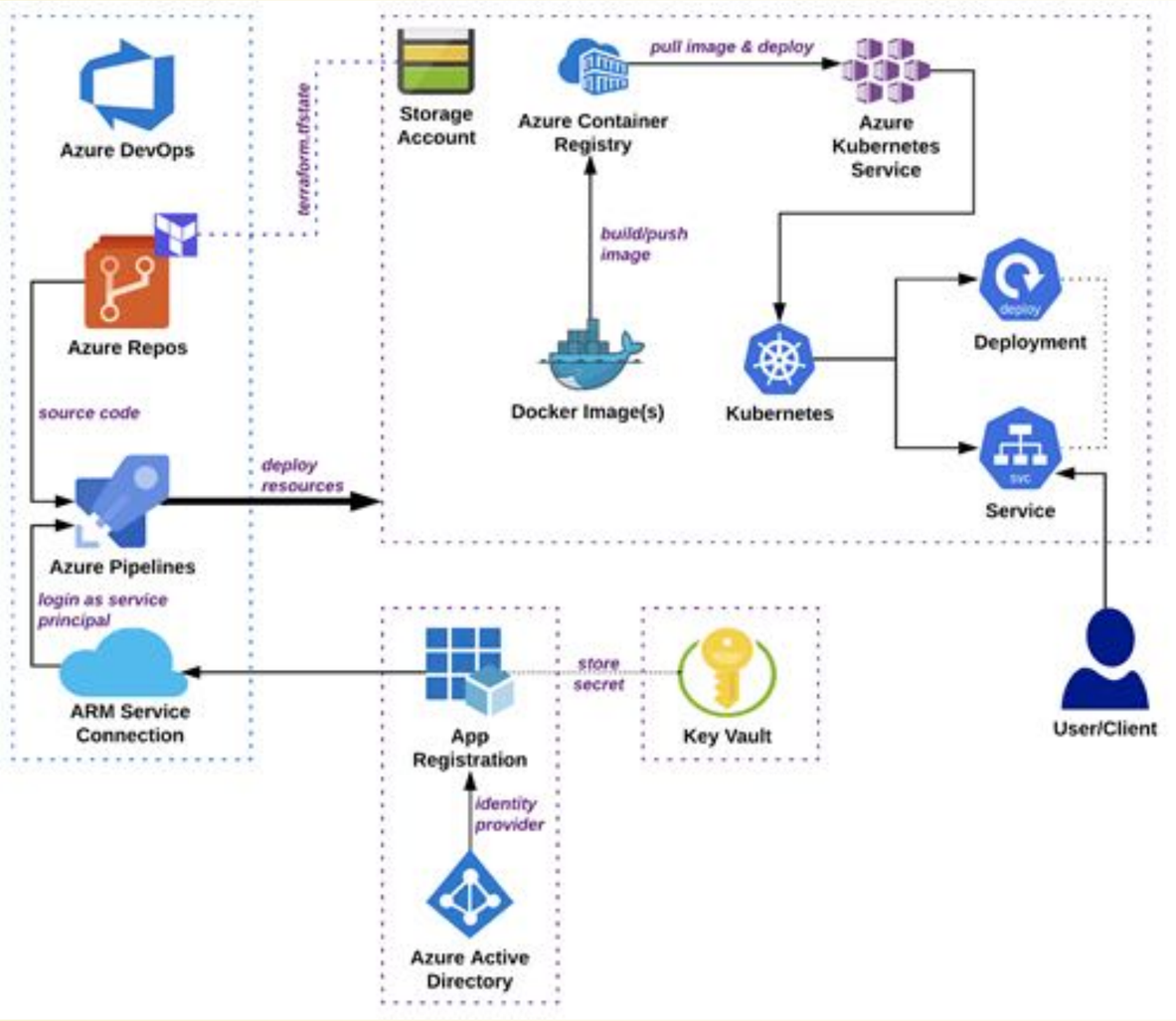
參考資料：Kubernetes Namespaces - Imperative using kubectl

Azure Monitor



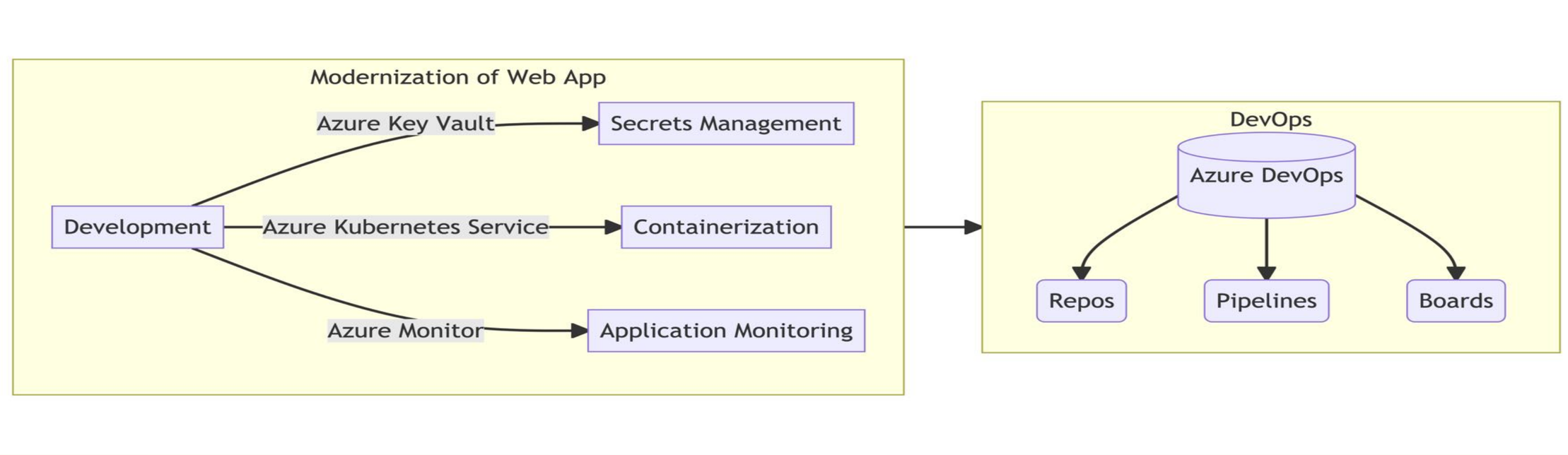
參考資料：Web application monitoring on Azure

Typical Cloud Native Architecture



參考資料：How To Deploy An Application Using The Azure Kubernetes Service

Dev -> Modernization -> DevOps



Trigger #2

ISO 27001

Scope = Infrastructure + Development + Product

afaq
ISO/IEC 27001
Information Security
AFNOR CERTIFICATION

afaq
AFNOR CERTIFICATION

Certificat
Certificate

N° 2021/94228.1

AFNOR Certification certifies that the management system implemented by:
AFNOR Certification certifie que le système de management mis en place par :

CALOUDI CORPORATION
卡洛地股份有限公司

for the following activities:
pour les activités suivantes :

[redacted]

has been assessed and found to meet the requirements of:
a été évalué et jugé conforme aux exigences requises par :

NF EN ISO/IEC 27001:2017 (Europe) - ISO/IEC 27001:2013 + COR 1:2014 + COR 2:2015 (International)

and is developed on the following locations:
et est déployé sur les sites suivants :

11F.-2, NO.89, SONGREN RD., XINYI DIST., TAIPEI CITY 110413,TAIWAN (R.O.C)
臺北市信義區松仁路 89 號 11 樓之 2

This certificate is valid from (year/month/day) / *Ce certificat est valable à compter du (année/mois/jour)* 2021-09-11 until / *jusqu'au* 2024-09-10

cofrac
CERTIFICATION DE SYSTÈMES DE MANAGEMENT

Julien NIZRI
Managing Director of AFNOR Certification
Directeur Général d'AFNOR Certification

Scan this QR code to check the validity of the certificate

11 rue Francis de Pressensé - 93571 La Plaine Saint-Denis Cedex - France - T. +33 (0)1 41 62 80 00 - F. +33 (0)1 49 17 90 00
SAS au capital de 18 187 000 € - 479 076 002 RCS Bobigny - www.afnor.org

afnor GROUPE 法國標準協會(AFNOR)艾法諾集團
—台灣區代表 貝爾國際驗證機構

驗證審查結果通知書
Review result notification

File No. 4218601

日期：2022年7月21日

敬致 公司/單位名稱：卡洛地股份有限公司

管理代表/負責人：[redacted] 先生

審查結果：

貴公司於 2022-07-11

執行 NF EN ISO/IEC 27001:2017(Europe)-ISO/IEC 27001:2013+COR 1:2014+COR 2:2015 (International) 驗證審查，經艾法諾集團 驗證經理審查結果如下：(打V者)

- ■ 矯正措施符合驗證標準要求。
- □ 現場稽核未發現不符合項目。
  - 經驗證決定小組核定：
  - □ 予以發證。
  - ■ 此次驗證通過，證書持續有效。
- □ 經現場查核，尚未符合驗證標準要求，本公司需再赴現場進行複查，複查計畫將另行通知。

貝爾國際驗證機構
系統管理部

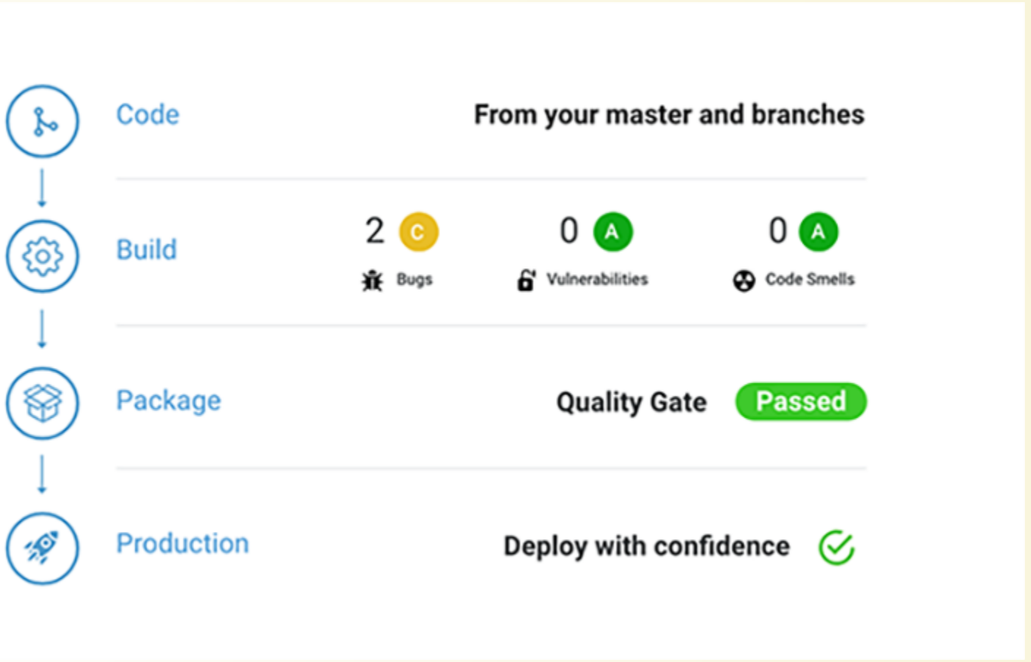
INST-4-1-1 Rev12-Sep.-2014

afaq 從企業的國際驗證 到永續經營…
從主管的管理啟蒙 到人才培育…
NF

Source Code Analysis

Static Analysis

- SQL Injection
- Cross-Site Scripting
- 有 Passive 也有 Aggressive 的作法



Dynamic Analysis

- Penetration Test
- 因爲要花比較多時間，通常不會每次 Check in 或是 Deploy 都做
- Report 出來就是以天或週爲單位，出來之後還要 Fix 也是以天或週爲單位

Azure Devops 可以整合 SonarQube。

參考資料：SonarQube

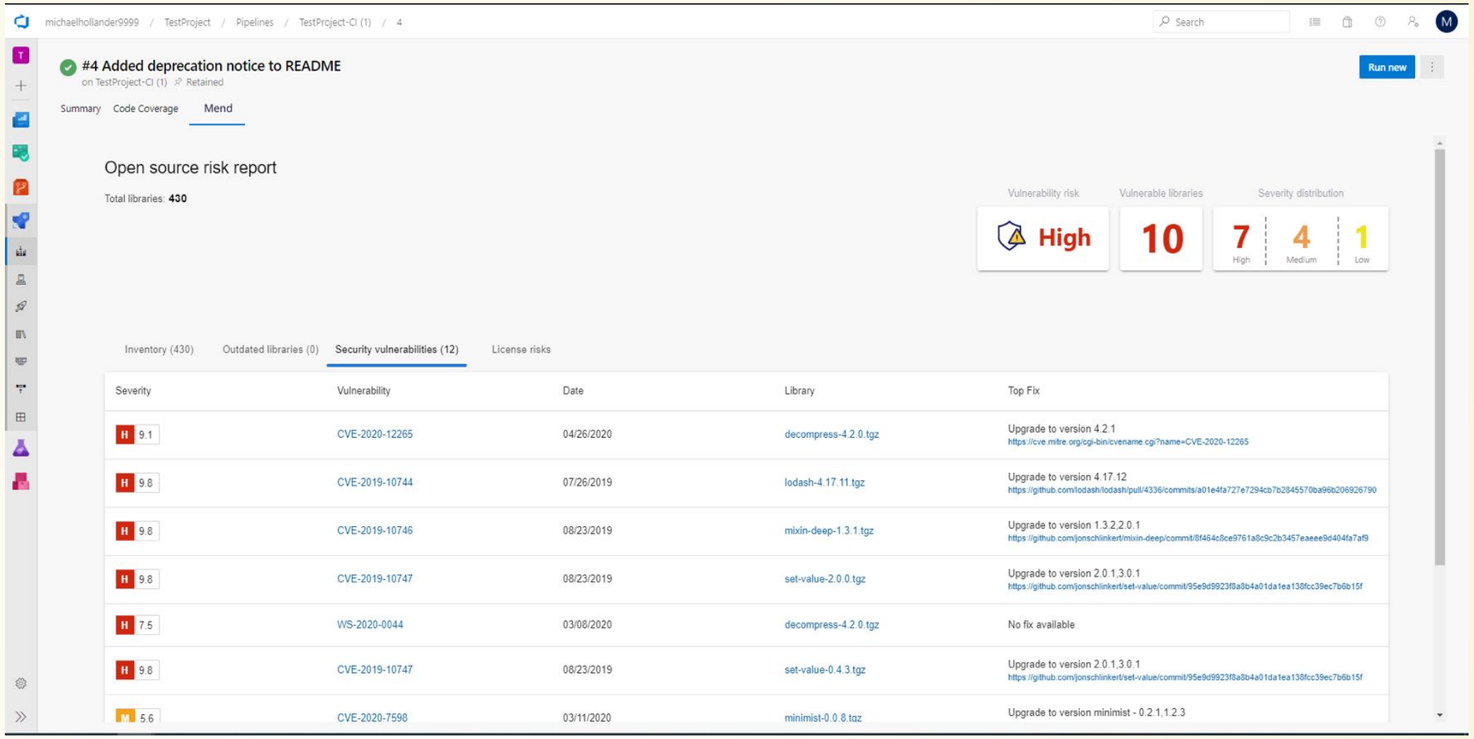
Software Composition Analysis

Code Analysis of

- Open Source Component
- 3rd-Party Library

For

- Vulnerability
- Outdated Component
- License Issue



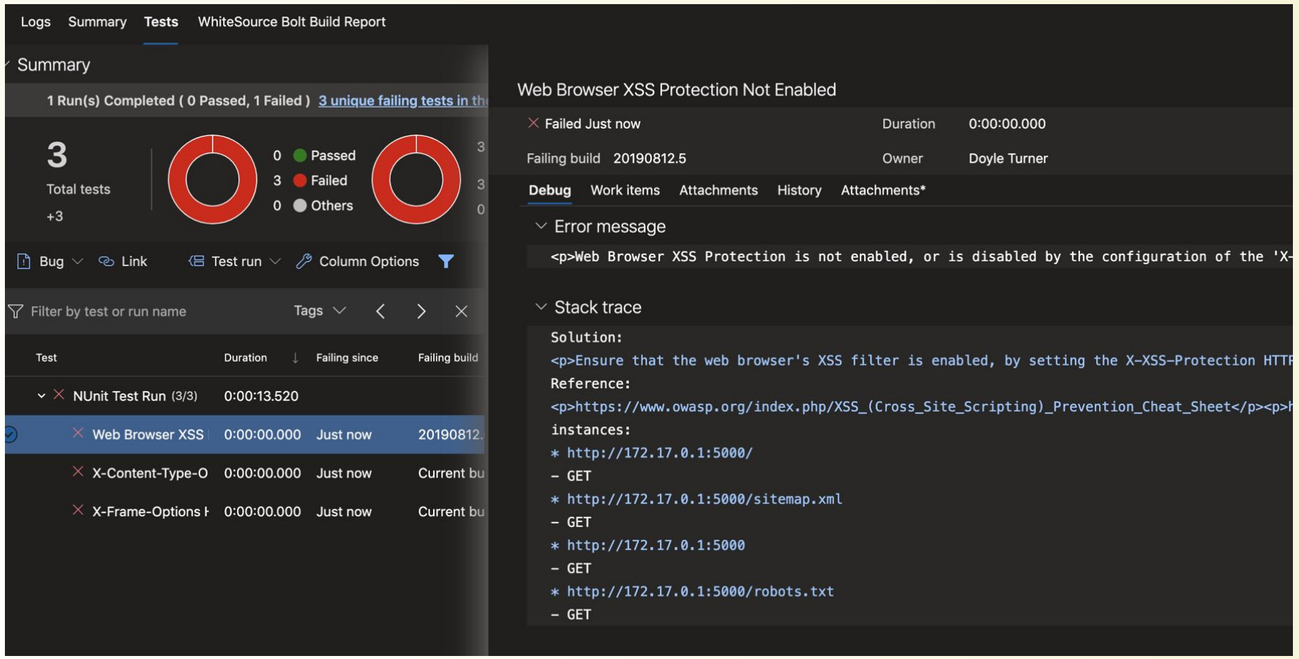
Azure DevOps 可以整合 WhiteSource Bolt (現在改名爲 Mend Bolt)。

參考資料：Mend Bolt (formerly WhiteSource)

Environment Security

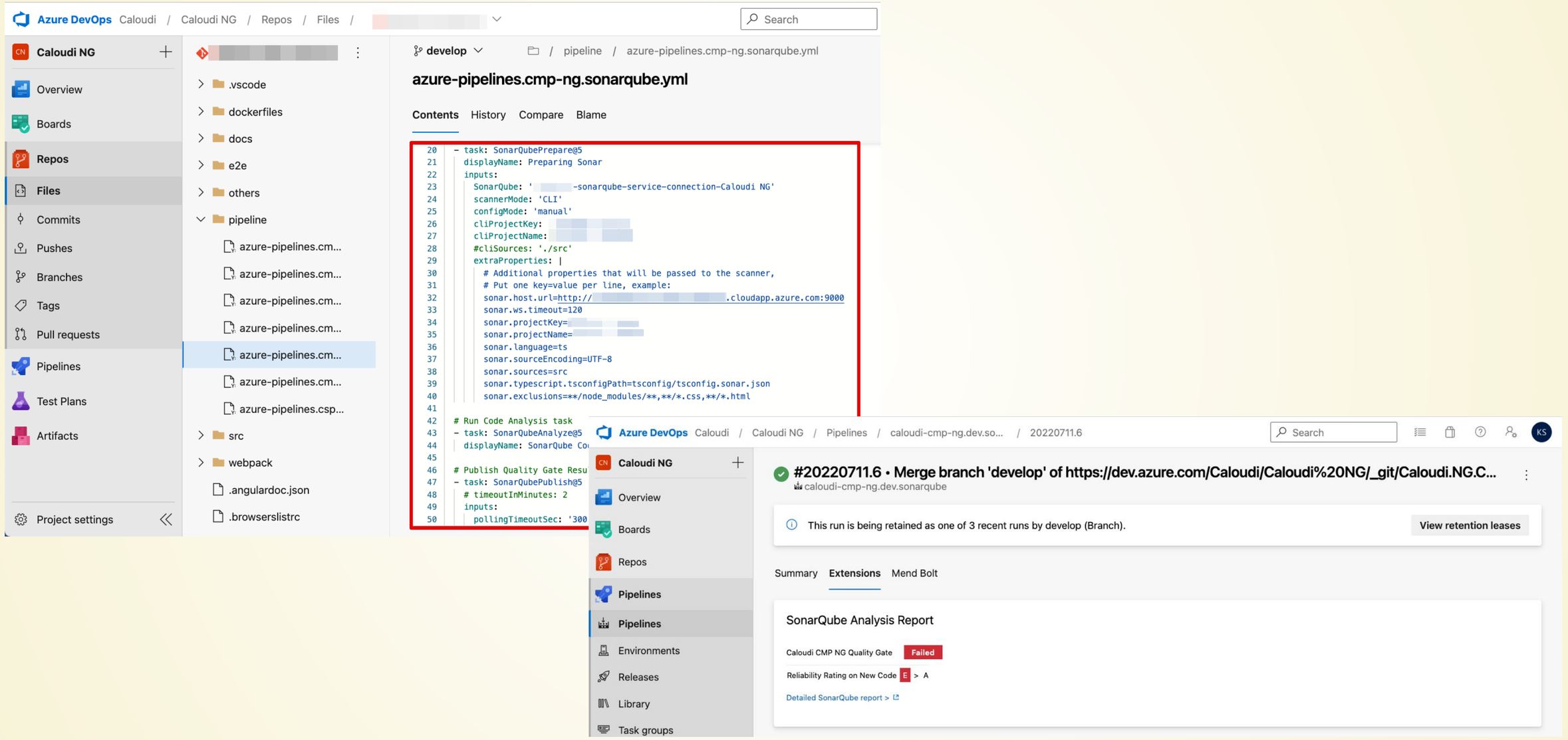
- Network Security Group (NSG)
- Azure Policies
- Role-Based Access Control (RBAC)
- Web Application Firewall (WAF)
- Azure Monitor

Azure Devops 可以整合 OWASP ZAP。

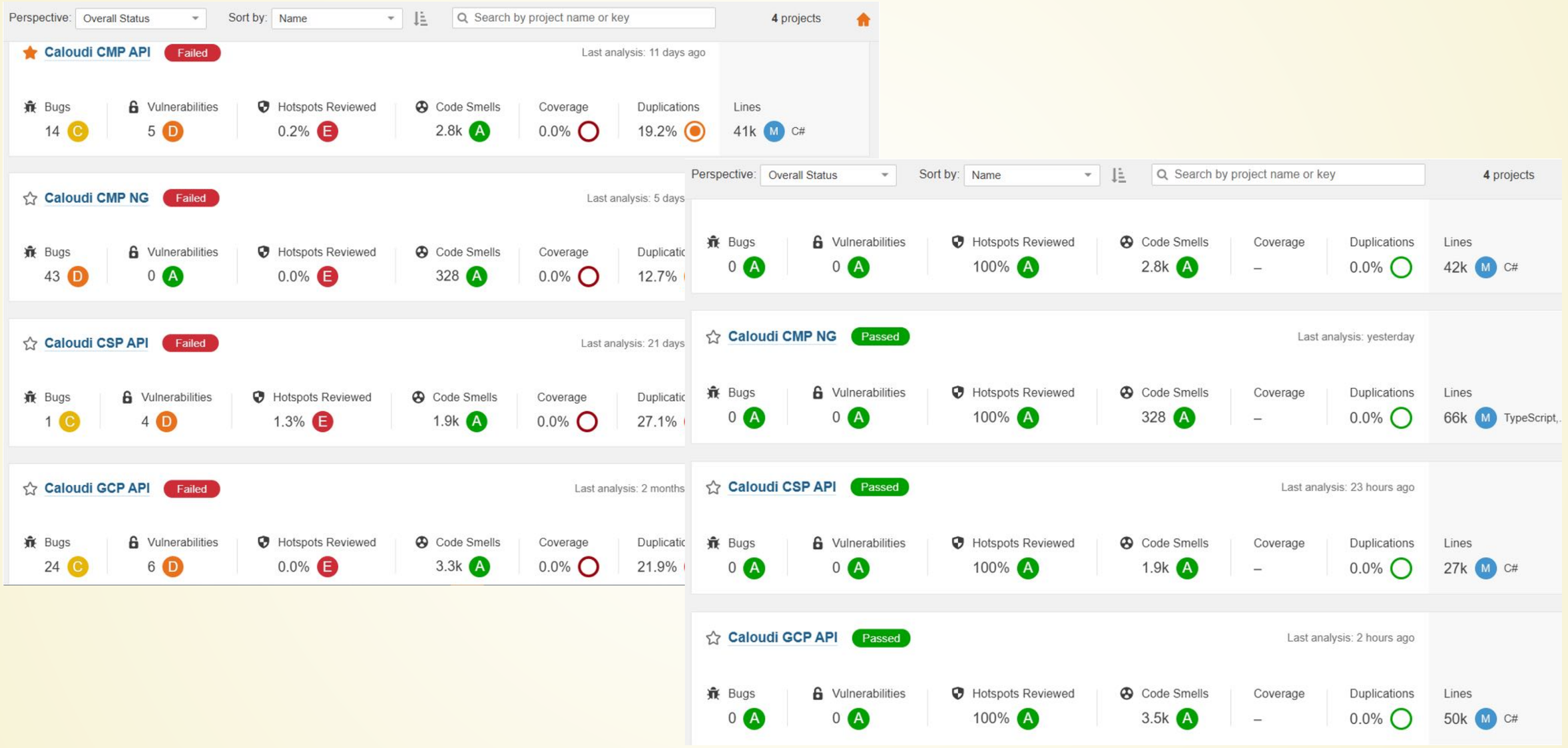


參考資料：OWASP/ZAP Scanning extension for Azure DevOps
參考資料：Running OWASP ZAP in Azure Kubernetes Service

SonarQube


Azure DevOps Caloudi / Caloudi NG / Repos / Files /
Search
Caloudi NG
Overview
Boards
Repos
Files
Commits
Pushes
Branches
Tags
Pull requests
Pipelines
Test Plans
Artifacts
Project settings
.vscode
dockerfiles
docs
e2e
others
pipeline
azure-pipelines.cm...
azure-pipelines.csp...
src
webpack
.angulardoc.json
.browserslistrc
develop
pipeline / azure-pipelines.cmp-ng.sonarqube.yml
azure-pipelines.cmp-ng.sonarqube.yml
Contents History Compare Blame
- task: SonarQubePrepare@5
displayName: Preparing Sonar
inputs:
SonarQube: '-sonarqube-service-connection-Caloudi NG'
scannerMode: 'CLI'
configMode: 'manual'
cliProjectKey:
cliProjectName:
#cliSources: './src'
extraProperties: |
# Additional properties that will be passed to the scanner,
# Put one key=value per line, example:
sonar.host.url=http://.cloudapp.azure.com:9000
sonar.ws.timeout=120
sonar.projectKey=
sonar.projectName=
sonar.language=ts
sonar.sourceEncoding=UTF-8
sonar.sources=src
sonar.typescript.tsconfigPath=tsconfig/tsconfig.sonar.json
sonar.exclusions=**/node_modules/**,**/*.css,**/*.html
# Run Code Analysis task
- task: SonarQubeAnalyze@5
displayName: SonarQube Co
Publish Quality Gate Resu
- task: SonarQubePublish@5
timeoutInMinutes: 2
inputs:
pollingTimeoutSec: '300
Azure DevOps Caloudi / Caloudi NG / Pipelines / caloudi-cmp-ng.dev.so... / 20220711.6
Search
KS
Caloudi NG
Overview
Boards
Repos
Pipelines
Pipelines
Environments
Releases
Library
Task groups
#20220711.6 • Merge branch 'develop' of https://dev.azure.com/Caloudi/Caloudi%20NG/_git/Caloudi.NG.C...
caloudi-cmp-ng.dev.sonarqube
This run is being retained as one of 3 recent runs by develop (Branch).
View retention leases
Summary Extensions Mend Bolt
SonarQube Analysis Report
Caloudi CMP NG Quality Gate
Failed
Reliability Rating on New Code
E
> A
Detailed SonarQube report >

Vulnerability Scan Report



WhiteSource Bolt

文件名稱：弱點處理報告單
文件編號：C-I-B-08-02　　版次：1.0

填表日期： 111 年 5 月 19 日　　紀錄編號：111-02

設備名稱		系統名稱	CMP 雲端管理平台	管理人員	
外部 IP		內部 IP		掃瞄時間	2022 年 5 月 19 日

項次	等級	弱點名稱	修補情形	修補日期	未修補原因說明與防禦因應方法
1	高	CVE-2021-22570 google.protobuf.3.13.0.nupkg	■已修補 □暫不修補	111/5/19	從 3.13.0 更新至 3.15.0 版本之後，問題即解決。
2	高	CVE-2019-0820 system.text.regularexpressions 4.3.1	□已修補 ■暫不修補	111/5/19	目前已經是建議的 4.3.1 版本，但是並未解決，不過每個 Endpoint 都會透過 FluentValidation 進行 Input Validation。
			□已修補 □暫不修補		
			□已修補 □暫不修補		
			□已修補 □暫不修補		
覆核單位					
負責人簽章			權責單位 主管簽章		

（註：等級為：風險等級「高」、「中」、「低」）

原始碼程式弱點掃描(修補前)：

1

本文件為卡洛地股份有限公司專有之財產，非經書面許可，不得透露或使用本文件，亦不得複印，複製或轉變成任何其他形式使用。

Open source risk report

Total libraries: **263**

Vulnerability risk	Vulnerable libraries	Severity distribution		
High	3	2 High	1 Medium	0 Low

Inventory (263)　Outdated libraries (0)　Security vulnerabilities (3)　License risks

Severity	Vulnerability	Date	Library	Top Fix
HIGH 7.5	CVE-2021-22570	2022-01-26	google.protobuf.3.13.0.nupkg	Upgrade to version Google.Protobuf - 3.15.0 https://github.com/protocolbuffers/protobuf/releases/tag/v3.15.0
HIGH 7.5	CVE-2019-0820	2019-05-16	system.text.regularexpressions.4.3.1.nupkg	Upgrade to version System.Text.RegularExpressions - 4.3.1 https://github.com/advisories/GHSA-cmhx-cq75-c4mj
MEDIUM 5.5	CVE-2021-34532	2021-08-12	microsoft.aspnetcore.authentication.jwtbearer.3.1.4.nupkg	Upgrade to version Microsoft.AspNetCore.Authentication.JwtBearer - 2.1.30, 3.1.18, 5.0.9 https://github.com/advisories/GHSA-q7cg-43mg-qp69

Open source risk report

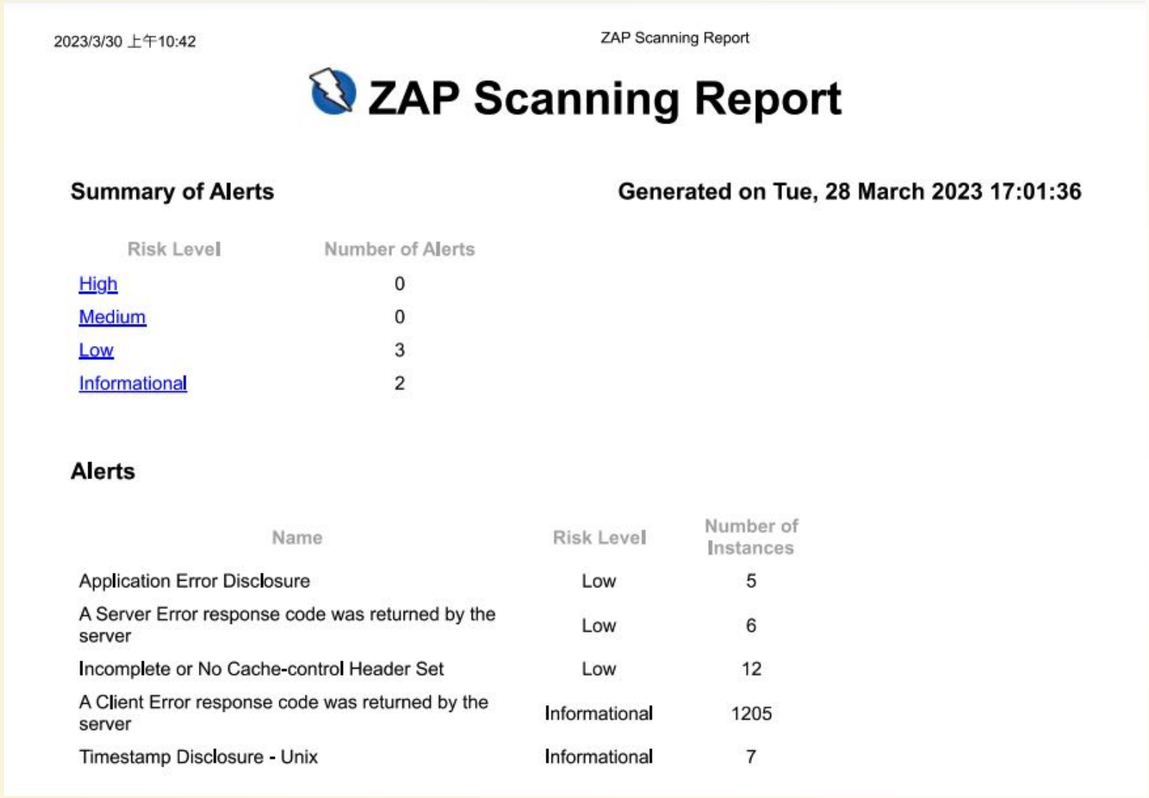
Total libraries: **264**

Vulnerability risk	Vulnerable libraries	Severity distribution		
High	2	1 High	1 Medium	0 Low

Inventory (264)　Outdated libraries (0)　Security vulnerabilities (2)　License risks

Severity	Vulnerability	Date	Library	Top Fix
HIGH 7.5	CVE-2019-0820	2019-05-16	system.text.regularexpressions.4.3.1.nupkg	Upgrade to version System.Text.RegularExpressions - 4.3.1 https://github.com/advisories/GHSA-cmhx-cq75-c4mj
MEDIUM 5.5	CVE-2021-34532	2021-08-12	microsoft.aspnetcore.authentication.jwtbearer.3.1.4.nupkg	Upgrade to version Microsoft.AspNetCore.Authentication.JwtBearer - 2.1.30, 3.1.18, 5.0.9 https://github.com/advisories/GHSA-q7cg-43mg-qp69

ZAP Scan



2023/3/30 上午10:42 ZAP Scanning Report

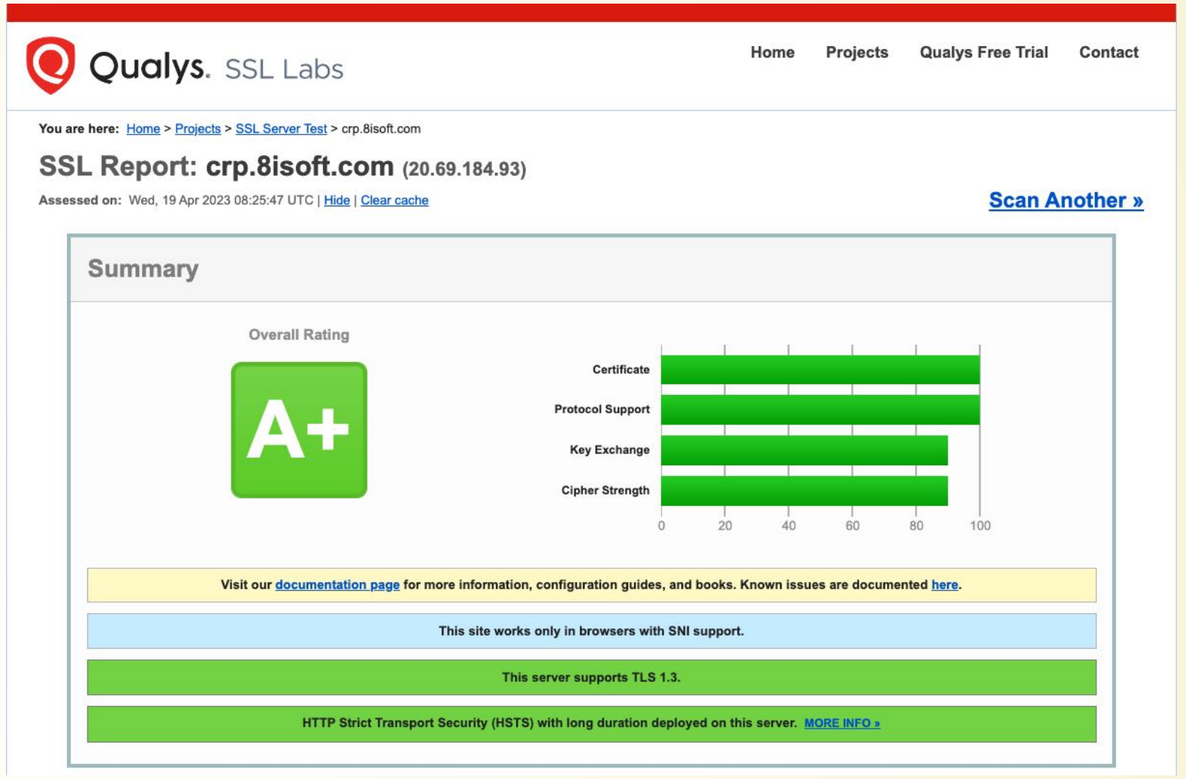
ZAP Scanning Report

Summary of Alerts **Generated on Tue, 28 March 2023 17:01:36**

Risk Level	Number of Alerts
High	0
Medium	0
Low	3
Informational	2

Alerts

Name	Risk Level	Number of Instances
Application Error Disclosure	Low	5
A Server Error response code was returned by the server	Low	6
Incomplete or No Cache-control Header Set	Low	12
A Client Error response code was returned by the server	Informational	1205
Timestamp Disclosure - Unix	Informational	7



Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

You are here: Home > Projects > SSL Server Test > crp.8isoft.com

SSL Report: crp.8isoft.com (20.69.184.93)

Assessed on: Wed, 19 Apr 2023 08:25:47 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

A+

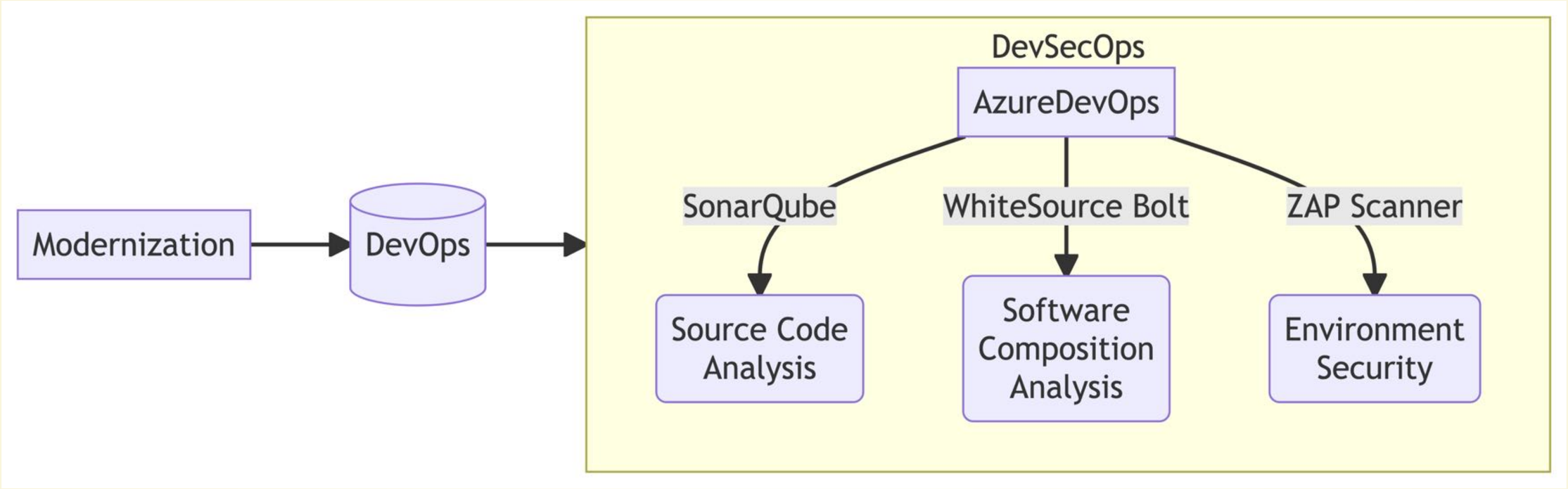
Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This site works only in browsers with SNI support.

This server supports TLS 1.3.

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »

Dev -> Modernization -> DevOps -> DevSecOps



參考資料：Time-Series Anomaly Detection Service at Microsoft

Trigger #3

ISO 27001

Objective = Continuous Operation

afaq
ISO/IEC 27001
Information Security
AFNOR CERTIFICATION

afaq
AFNOR CERTIFICATION

Certificat
Certificate

N° 2021/94228.1

AFNOR Certification certifies that the management system implemented by:
AFNOR Certification certifie que le système de management mis en place par :

CALOUDI CORPORATION
卡洛地股份有限公司

for the following activities:
pour les activités suivantes :

[redacted]

has been assessed and found to meet the requirements of:
a été évalué et jugé conforme aux exigences requises par :

NF EN ISO/IEC 27001:2017 (Europe) - ISO/IEC 27001:2013 + COR 1:2014 + COR 2:2015 (International)

and is developed on the following locations:
et est déployé sur les sites suivants :

11F.-2, NO.89, SONGREN RD., XINYI DIST., TAIPEI CITY 110413,TAIWAN (R.O.C)
臺北市信義區松仁路 89 號 11 樓之 2

This certificate is valid from (year/month/day) / *Ce certificat est valable à compter du (année/mois/jour)* 2021-09-11 until / *jusqu'au* 2024-09-10

cofrac
CERTIFICATION DE SYSTÈMES DE MANAGEMENT

Julien NIZRI
Managing Director of AFNOR Certification
Directeur Général d'AFNOR Certification

Scan this QR code to check the validity of the certificate

11 rue Francis de Pressensé - 93571 La Plaine Saint-Denis Cedex - France - T. +33 (0)1 41 62 80 00 - F. +33 (0)1 49 17 90 00
SAS au capital de 18 187 000 € - 479 076 002 RCS Bobigny - www.afnor.org

afnor GROUPE 法國標準協會(AFNOR)艾法諾集團 —台灣區代表 貝爾國際驗證機構

驗證審查結果通知書
Review result notification

File No. 4218601

日期：2022年7月21日

敬致 公司/單位名稱：卡洛地股份有限公司

管理代表/負責人：[redacted] 先生

審查結果：

貴公司於 2022-07-11

執行 NF EN ISO/IEC 27001:2017(Europe)-ISO/IEC 27001:2013+COR 1:2014+COR 2:2015 (International) 驗證審查，經艾法諾集團 驗證經理審查結果如下：(打V者)

■ 矯正措施符合驗證標準要求。
☐ 現場稽核未發現不符合項目。
經驗證決定小組核定：
☐ 予以發證。
■ 此次驗證通過，證書持續有效。
☐ 經現場查核，尚未符合驗證標準要求，本公司需再赴現場進行複查，複查計畫將另行通知。

貝爾國際驗證機構
系統管理部

INST-4-1-1 Rev12-Sep.-2014

afaq 從企業的國際驗證 到永續經營…
從主管的管理啟蒙 到人才培育…
NF

Disaster Recovery

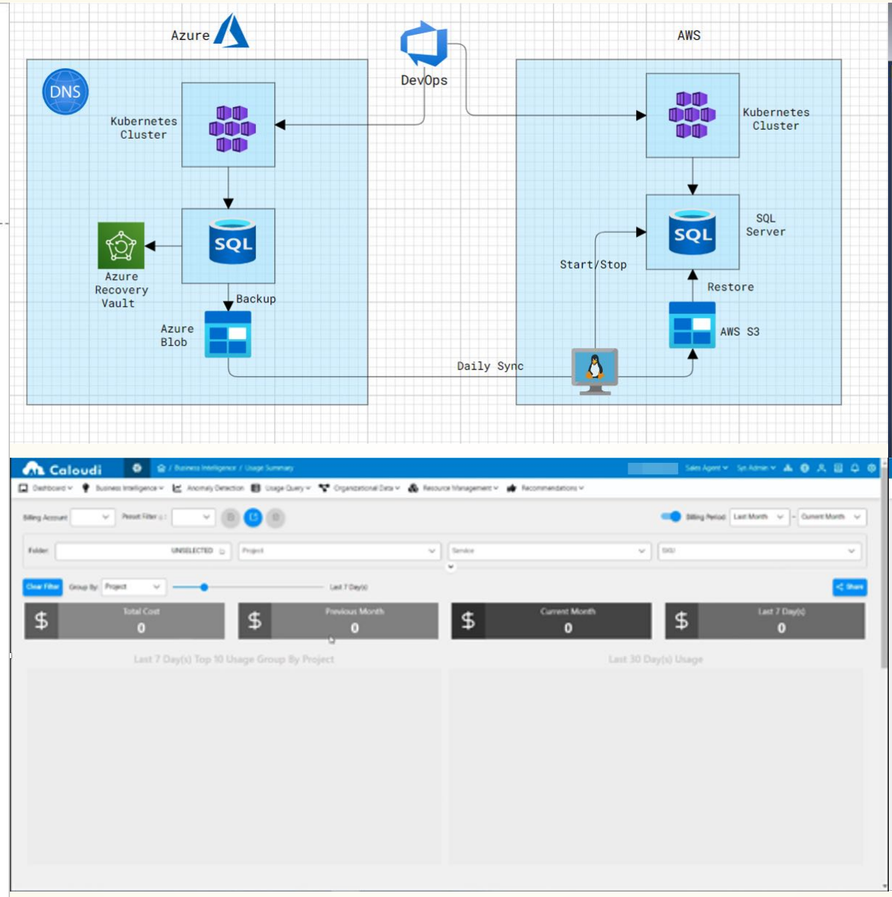
紀錄編號：111-01

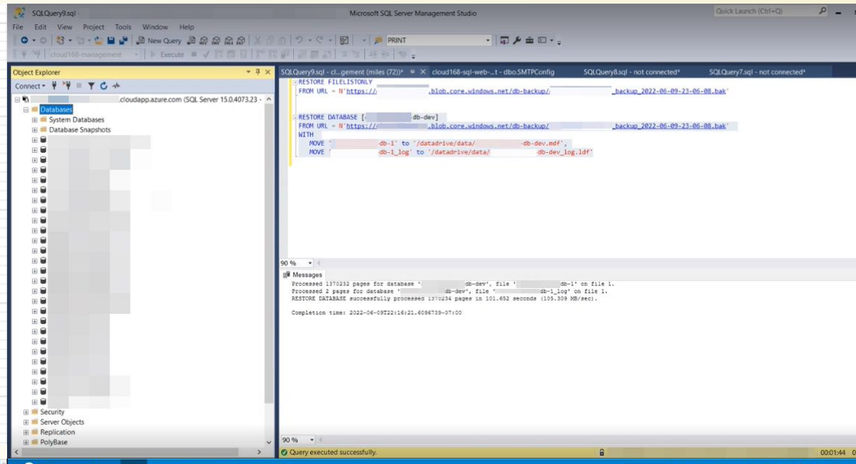
演 練 規 劃 表

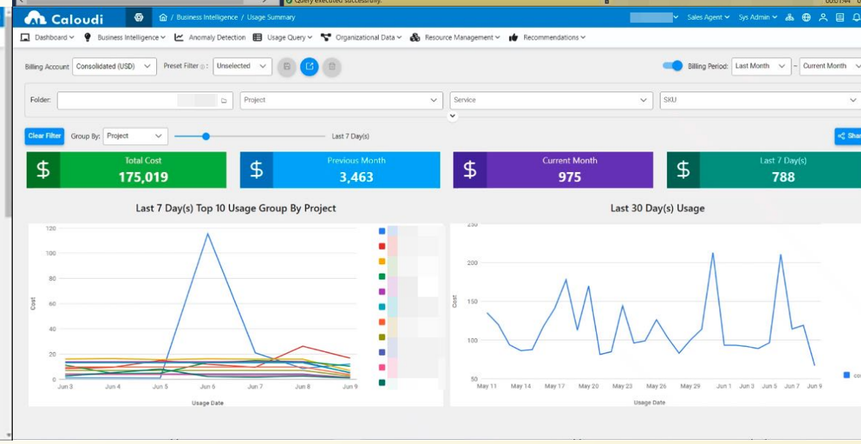
承辦單位/人員	資訊部/	協辦單位/人員	無
預計執行日期	111 年 6 月 10 日	填表日期	111 年 6 月 10 日

	演練規劃項目	規劃內容
1	規劃演練目標與範圍	目標：災害復原 範圍：CMP 雲端管理平台資料庫毀損
2	規劃演練腳本	CMP 雲端管理平台出狀況，導致 BI Dashboard 資料有誤，檢查結果發現資料庫毀損，因此回復資料庫備份。
3	規劃演練所需設備	瀏覽器 網路
4	規劃演練所需系統	筆電一台
5	規劃演練所需參與人員	資訊部/
6	規劃演練時程及完成時限(完成時限參考衝擊分析)	預計開始時間：2022-06-10 13:00 預計完成時限：2022-06-10 13:30 因為是假想 CMP 雲端管理平台的資料庫出狀況進行災害復原，實際上 CMP 雲端管理平台一切正常，所以對 CMP 雲端管理平台使用客戶完全不會有任何影響。
7	規劃演練測試方式與測試資源(如：僅測試資料復原 / 兼測資料復原與系統復原 / 僅資訊處相關承辦參與測試 / 使用者參與測試)	測試資料復原
8	規劃演練成果的檢討時程	2022-06-10 14:00 - 14:30

權責單位承辦人員		資訊權責單位主管		權責單位主管	





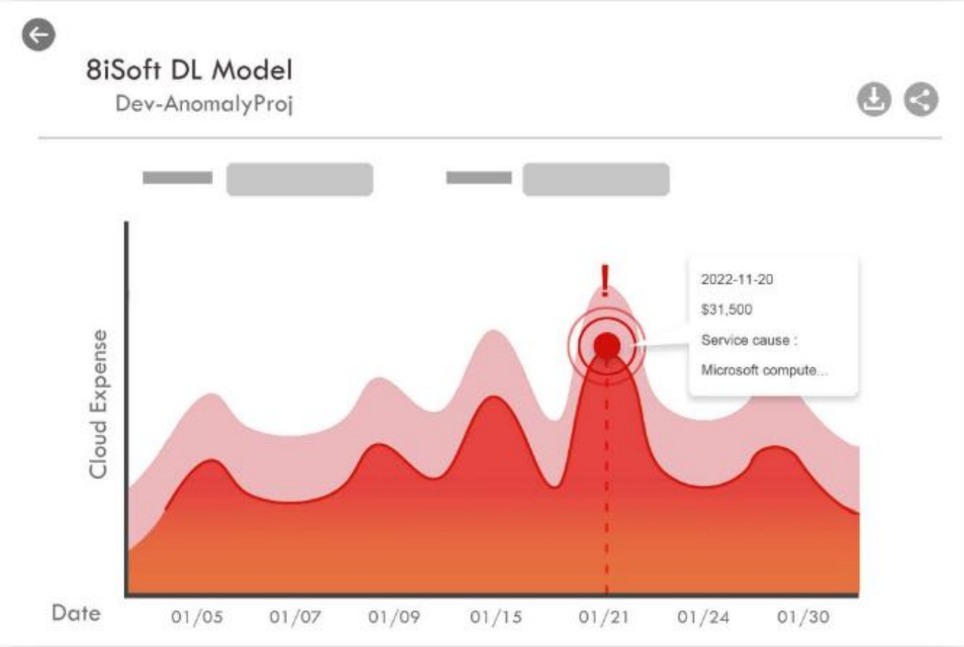


雲端費用 Anomaly Detection

8iSoft Pricing Contact Us English CRP Login

Resource Monitoring and Planning

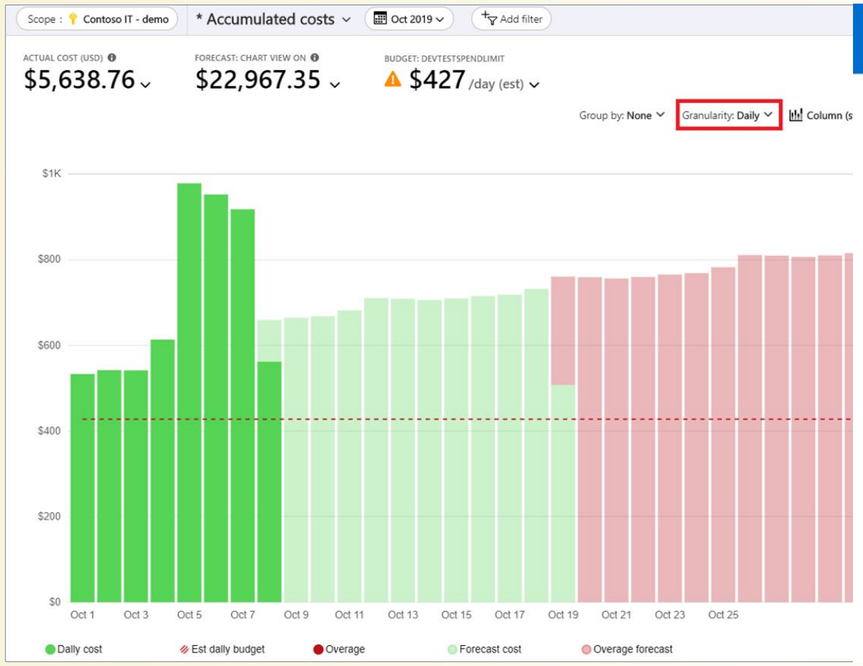
AI Monitor | Allocation Recommendation | Budgeting

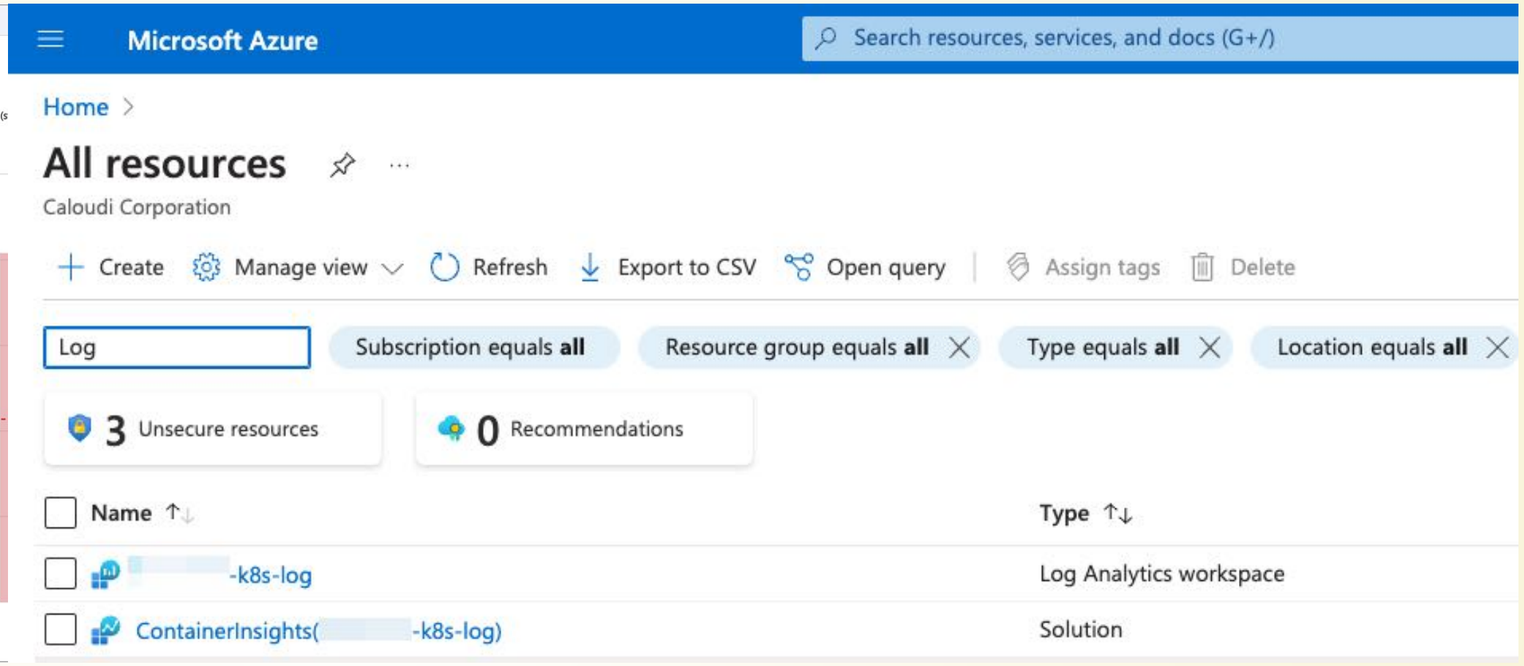


AI Monitor

- Top anomalies alerted in Advisor Dashboard
- Click alert card to pin-point primary causes from service down to instance level
- Adjustable time frame and sensitivity level

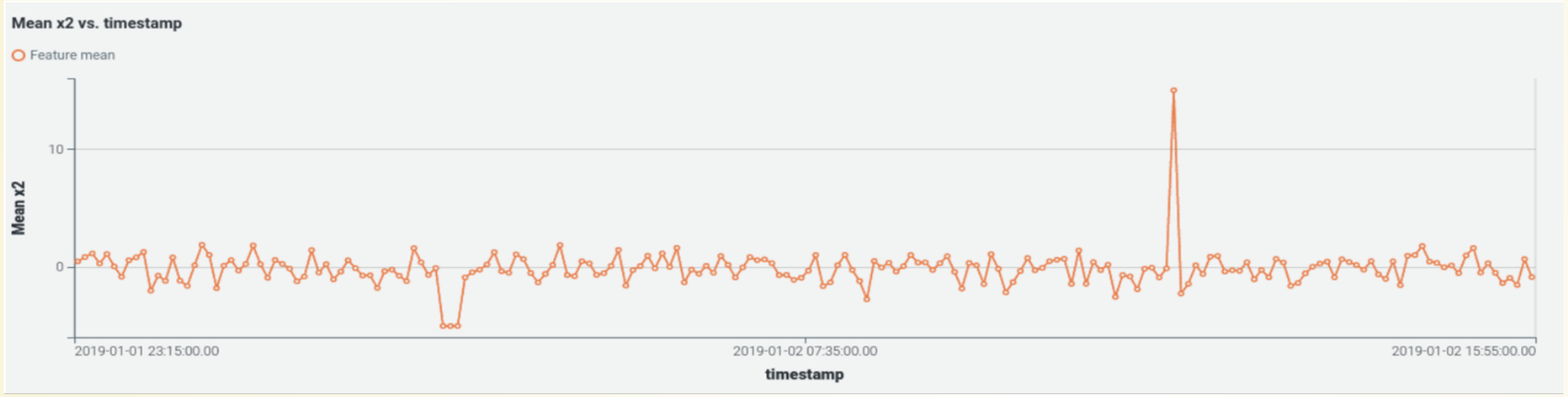
Billing Data / Log Data 都是 Time-Series Data

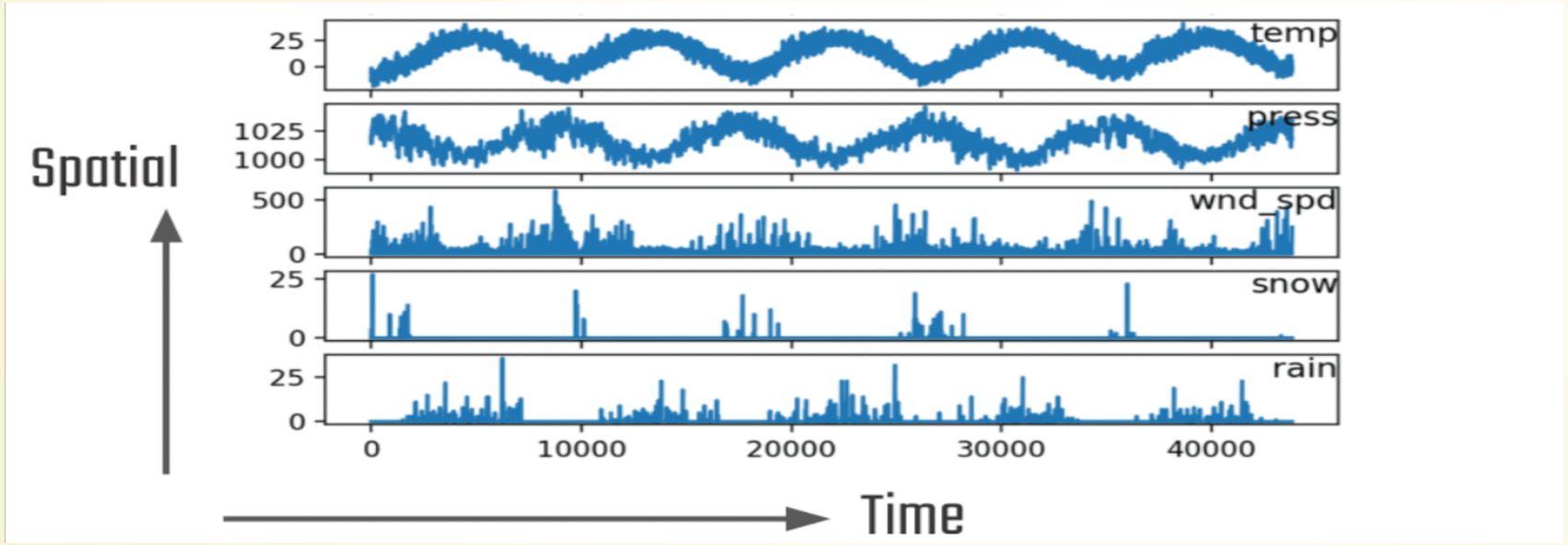




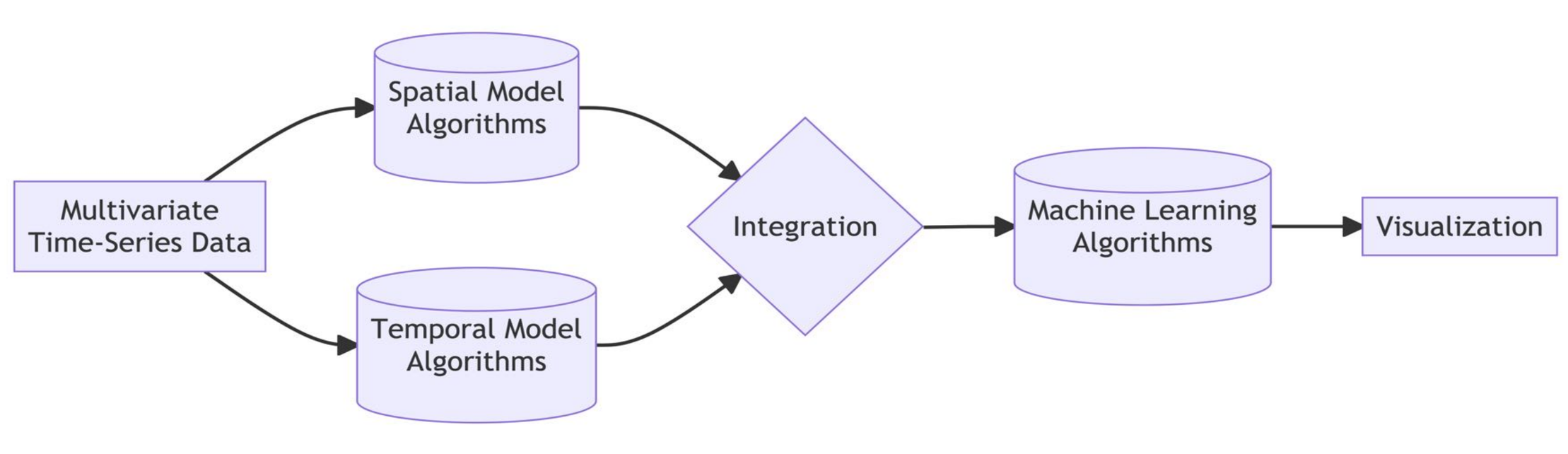
參考資料：Common cost analysis uses

Univariate / Multivariate Time-Series Data

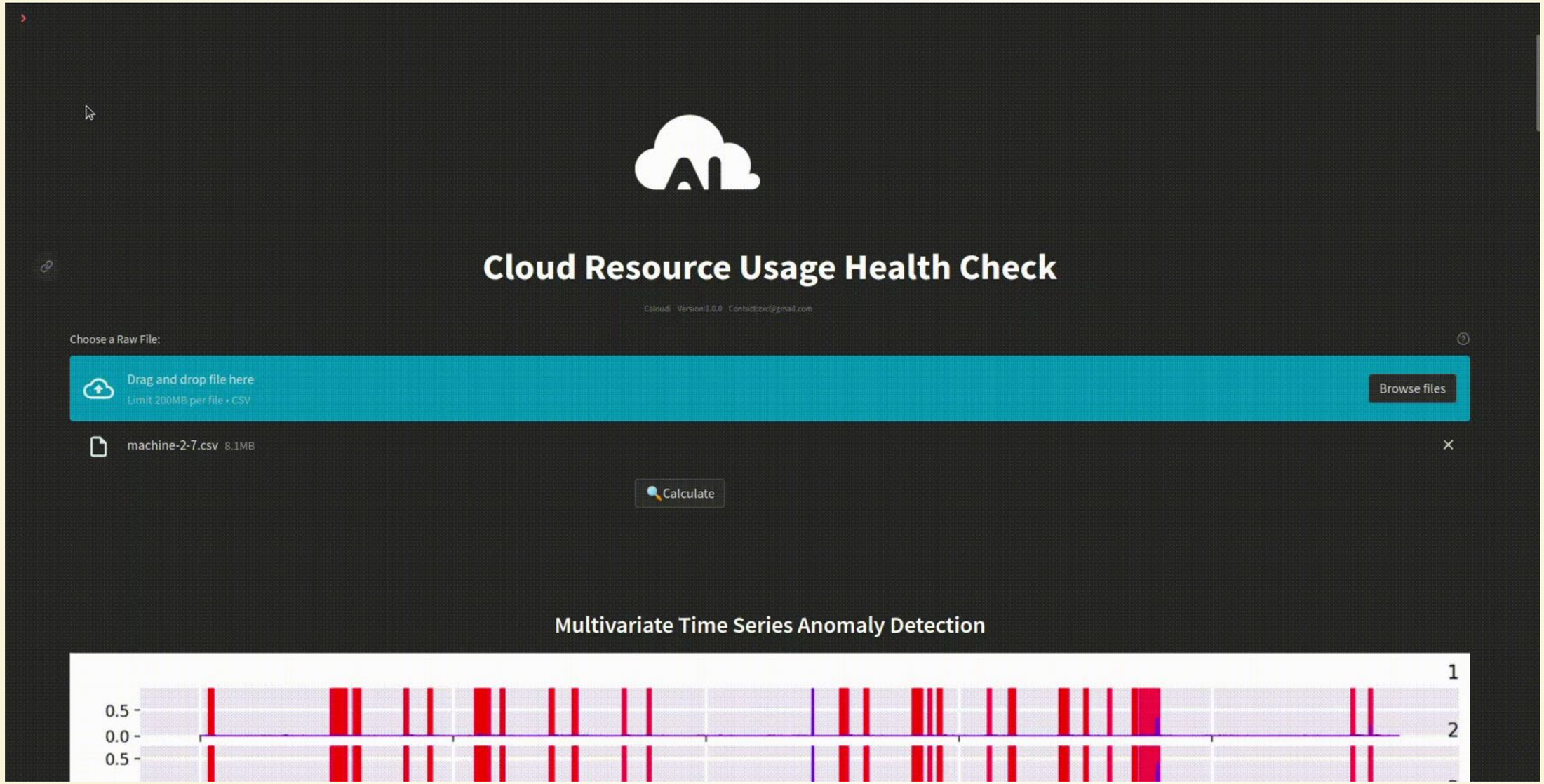




Machine Learning Model for Multivariate Time-Series Data Anomaly Detection



Cloud Resource Health Check



Multivariate Time-Series Data Anomaly Detection via Graph Attention Network

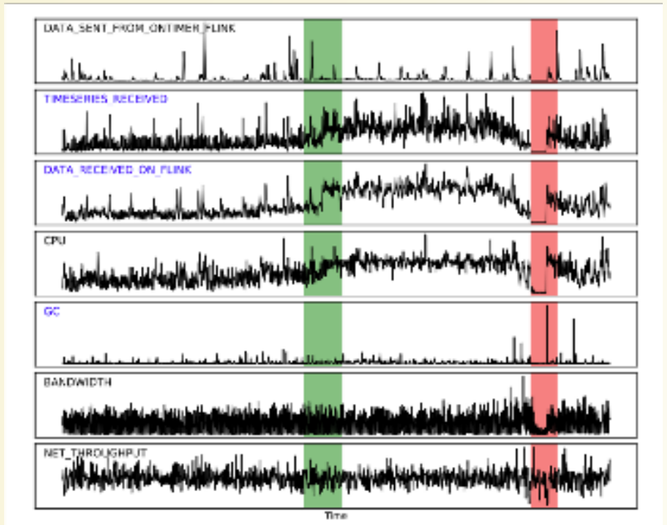


Fig. 1. An example of multivariate time-series input. Green indicates normal values and red indicates anomalies.

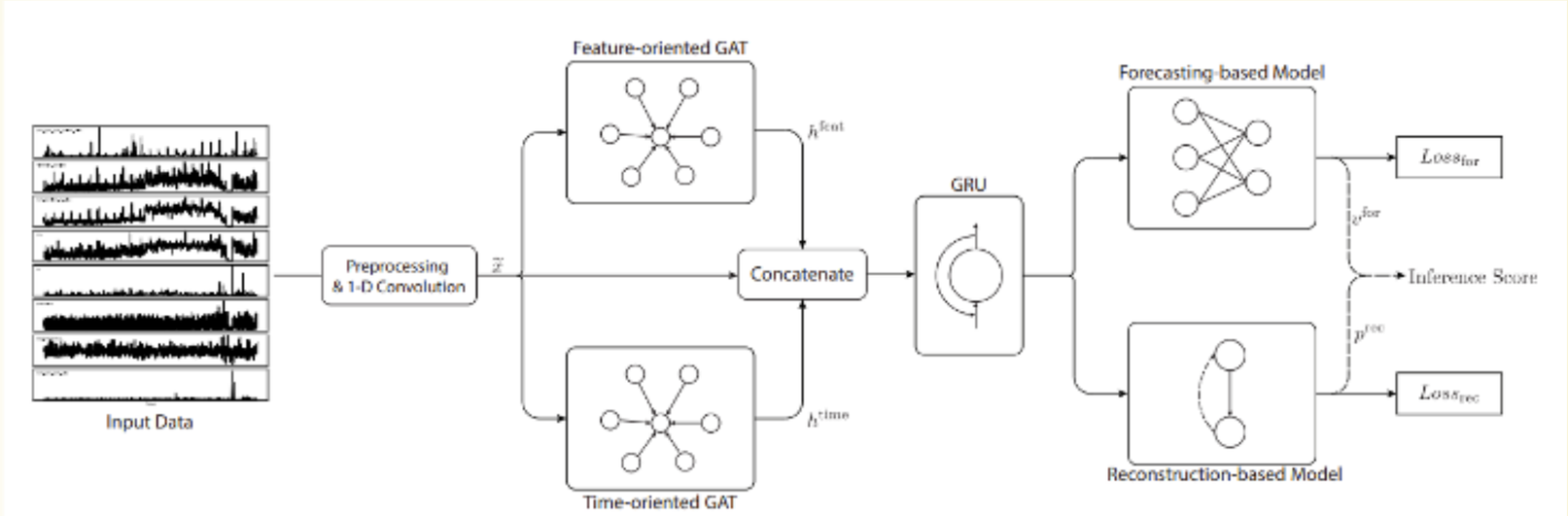
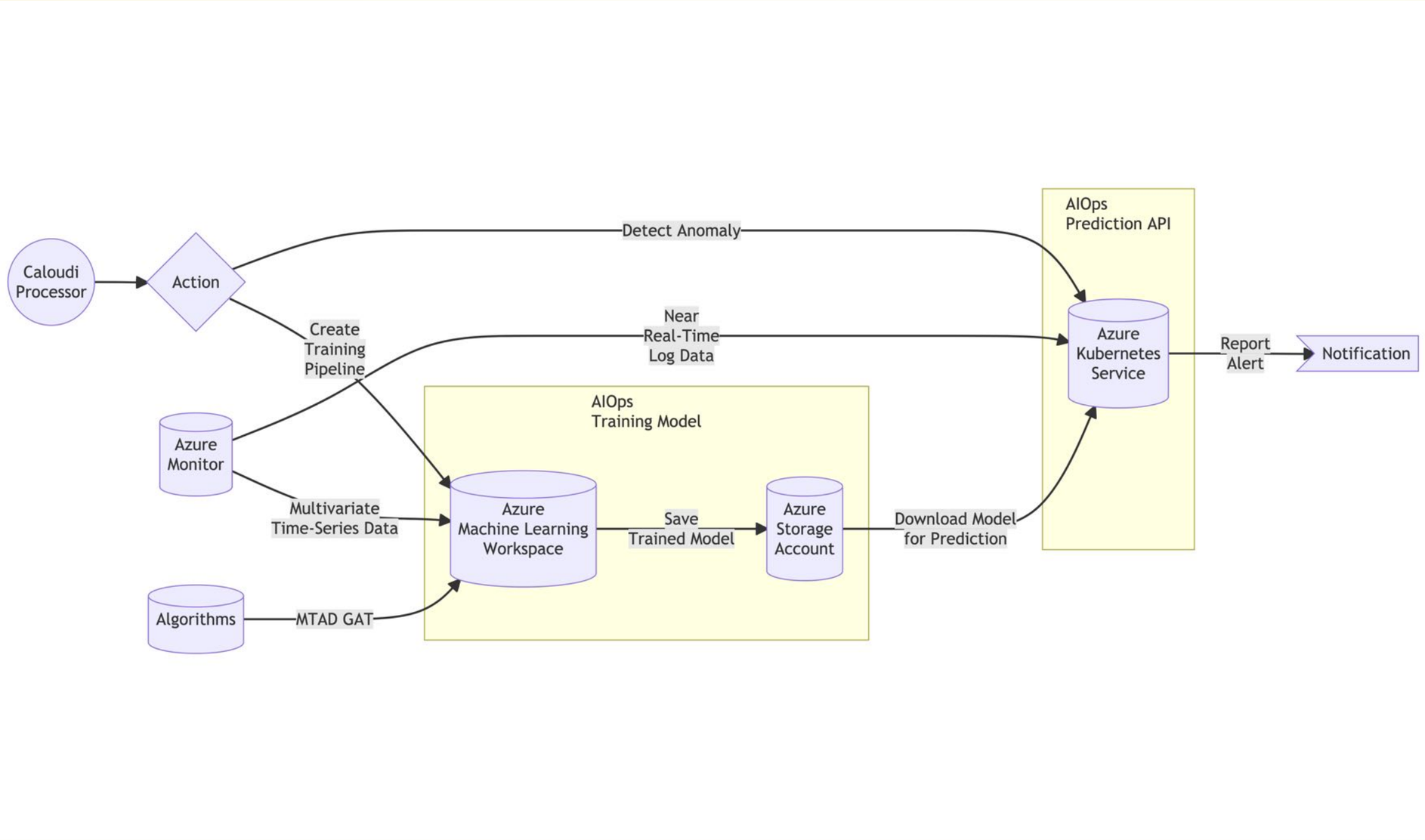


Fig. 2. The architecture of MTAD-GAT for multivariate time-series anomaly detection

參考資料：Multivariate Time-series Anomaly Detection via Graph Attention Network

Deep Learning Model for Multivariate Time-Series Data Anomaly Detection



Automated Alert Notification Report

8iSoft CRP Report

Automated Report

8iSoft CRP - Report: [redacted] 2023-04-16 22:17 (UTC)

Enrollment Number : 66247104

App Name : [redacted]

Report Id : 166341

Threshold : 0.47

{ "anomalyRecipients": [redacted],

"composition": [{ "instanceId": "/subscriptions/[redacted]

Composition : [redacted]/resourceGroups/[redacted]/providers/Microsoft.Compute/virtualMachines/[redacted]",

"resourceType": "virtualMachine", "poolName": "", "doDeeplog": false, "deeplogOSType": "windows",

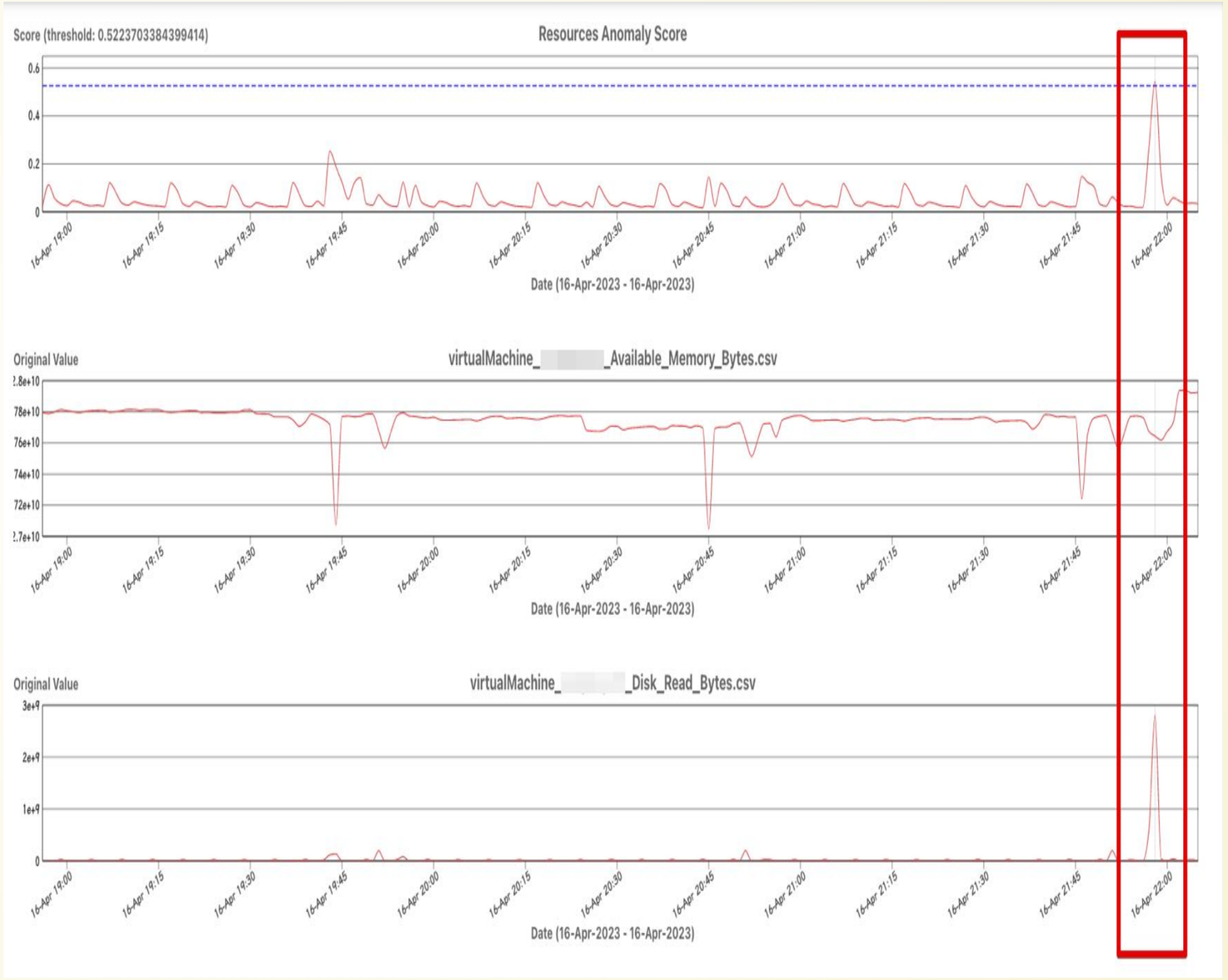
"doMATD": true }]}

Anomaly Time Stamps : ["04/16/2023 21:58:00"]

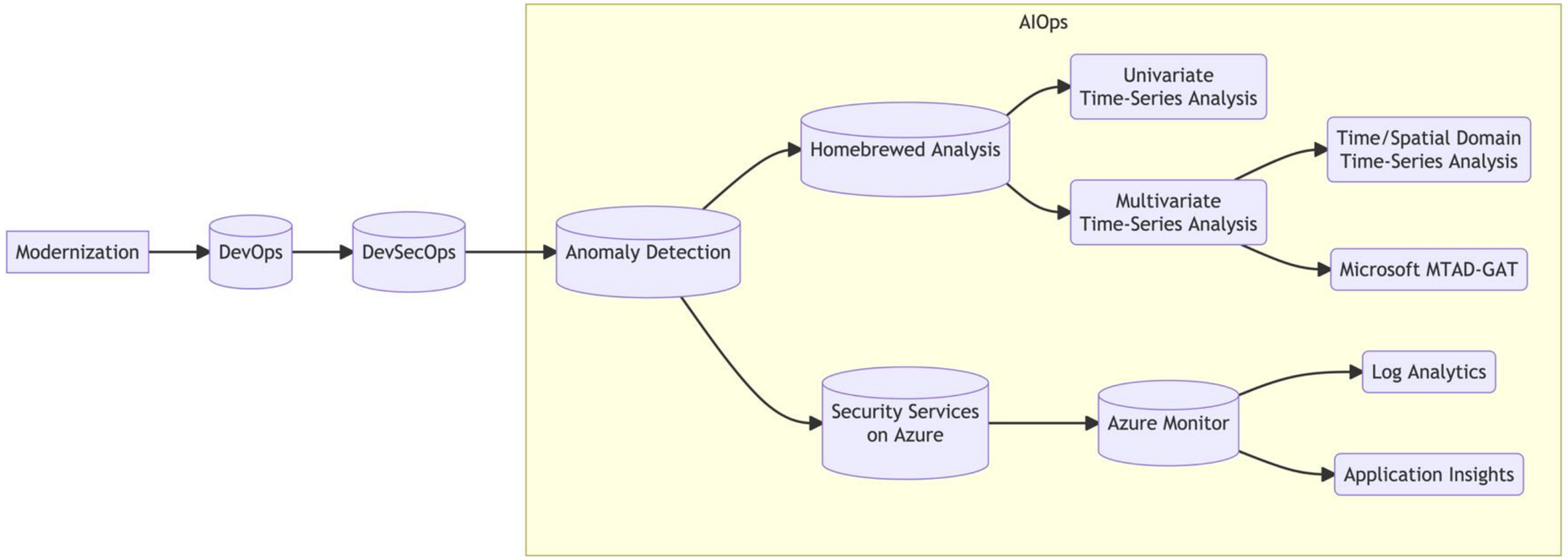
View Report

Sent by Cloud Resource Planning Platform

If you have any questions, please send to support.



Dev -> Modernization -> DevOps -> DevSecOps -> AIOps

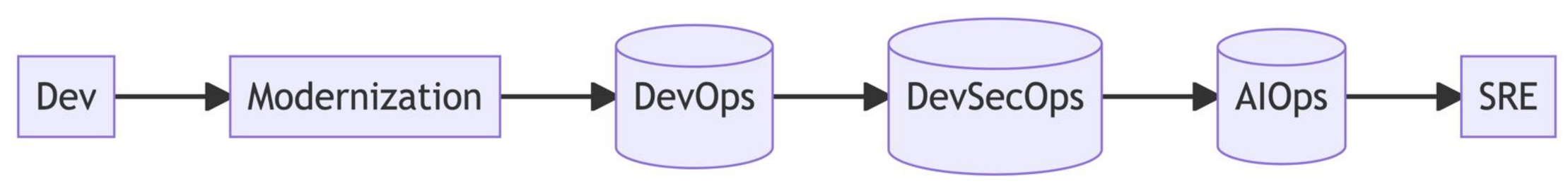


Why AIOps

- 人力難以掌控，AI 可以訓練。
- 可以運用人工智慧的時候，爲什麼要使用工人智慧？
- 費用
  - Training 一次大約 2 小時
    Azure Standard_NC6, 6 vCPUs, 56 GB RAM, 340 GB Temporary Storage
    NT$40.207/Hour
  - Prediction 一次大約 10 秒
    Azure Standard_D4as_v4, 4 vCPUs, 16 GB RAM, 32 GB Temporary Storage
    NT$6.818/Hour

Summary

Keypoints



- AI 的快速發展，讓無時無刻不斷記錄下來的維運資料，有了新的用途，那就是 AIOps。
- 從 Development 到 Deployment 到 Operation 一路下來，直接採用 Public Cloud 提供的 DevOps 服務快速建構維運平台的基礎設施，並且搭配適當的 Extension 補強 Security，迅速幫維運平台加開外掛，延伸到 DevSecOps 領域。
- 利用 Deep Learning 建構 Anomaly Detection Model，根據傳入的 Log Data 與 Performance Metrics 判斷是否有發生異常狀況的可能性，自動發出 Alert 通知 SRE 團隊，儘早發現，儘早修復。
- 將 AIOps 導入 SRE，提升維運的品質與效益，同時節省不必要的人力物力損耗。