

From AI to AIOps to SRE

~~ SRE Conference 2023 ~~

Kuo-Chun Su



Caloudi = Cloud + AI

Independent Software Vendor for Cloud Resource Planning and Cost Management

The screenshot displays the 8iSoft website interface. At the top, a dark teal banner reads "Now available on Azure Marketplace >>". The 8iSoft logo is on the left, with navigation links for "Pricing", "Contact Us", and "English" on the right. An orange "CRP Login" button is positioned in the top right corner. The main content area features a large heading "Saving More with Less" and a sub-heading "ACHIEVE 4X EFFICIENCY AND SAVE ¼ CLOUD COST". Below this, a paragraph describes the software's capabilities: "Plan your cloud resources at ease with 8iSoft CRP with RBAC, resource-tag-level analytics, AI-based alerts, and much more for you to explore." Two buttons, "Purchase Now" and "Why CRP ->", are located at the bottom left. On the right side, a dashboard preview is shown with a sidebar and a main content area. The dashboard includes a navigation menu with icons for home, menu, target, and refresh. The main content area has tabs for "Overall", "Azure", "GCP", and "AWS". It displays a pie chart for "Overall" (100%), a bar chart for "Monthly Cost", a line chart for "30 Day Potential Waste" (10%), and a world map. A table summarizes the cloud provider usage: Overall (100%), Azure (45%), GCP (25%), and AWS (30%).

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

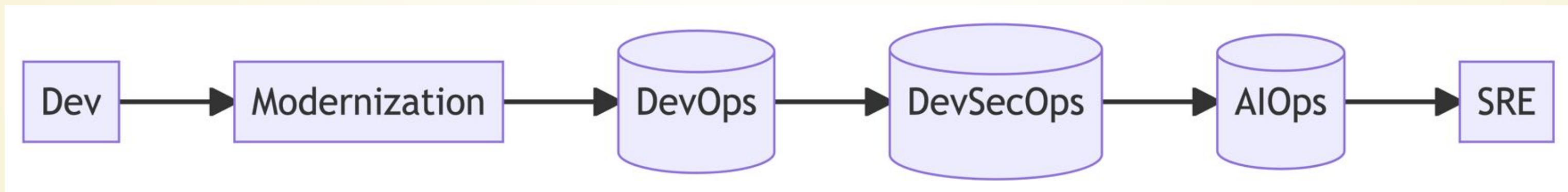
- 公司的弱電，是 CEO 買材料親自拉的。
- 公司的網路規劃跟有線網路配置，是 CEO 買材料親自佈線的。
- 公司的創意發想，是 CEO 跟 CTO 一起腦力激盪出來的。
- 公司的產品規劃跟實作，是 CTO 跟 RD Team 一起開發的。
- ...
- 在我出國休假的時候，CEO 把全公司的燈泡都換了。

在這種情況底下，身為 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，我們是怎麼因為各種需求，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：為了避免動搖國本，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：為了取信於大家必須放的真實圖片，會加上馬賽克之後，再放到投影片裡頭。

Trigger #1

Microsoft Cloud Partner Program



ADVANCED SPECIALIZATION

Windows Server and SQL Server Migration to Azure

Linux and Open Source Databases Migration to Azure

Modernization of Web Applications in Azure

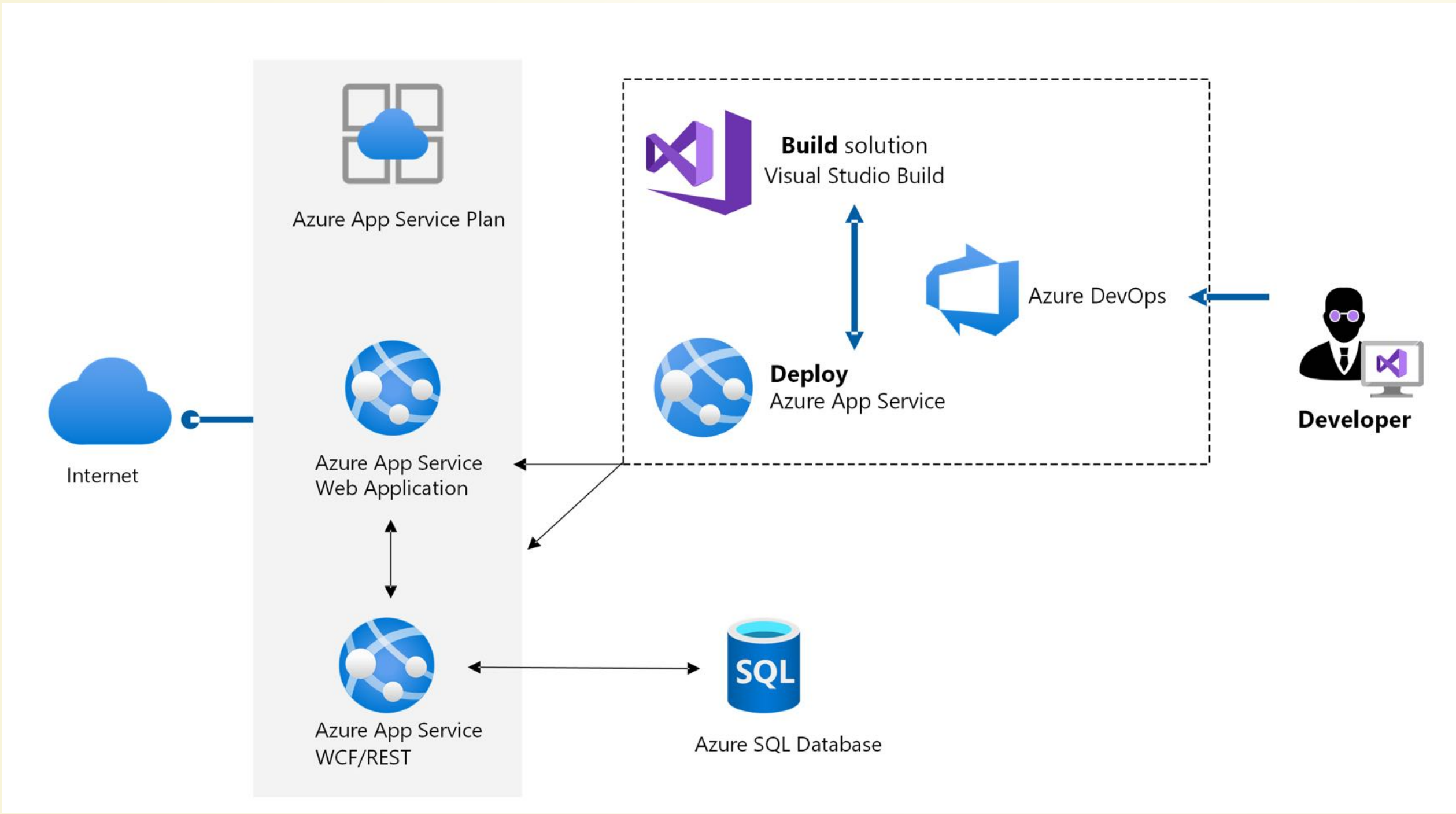
Analytics on Microsoft Azure



Gold
Microsoft Partner



Original .NET Core Web App

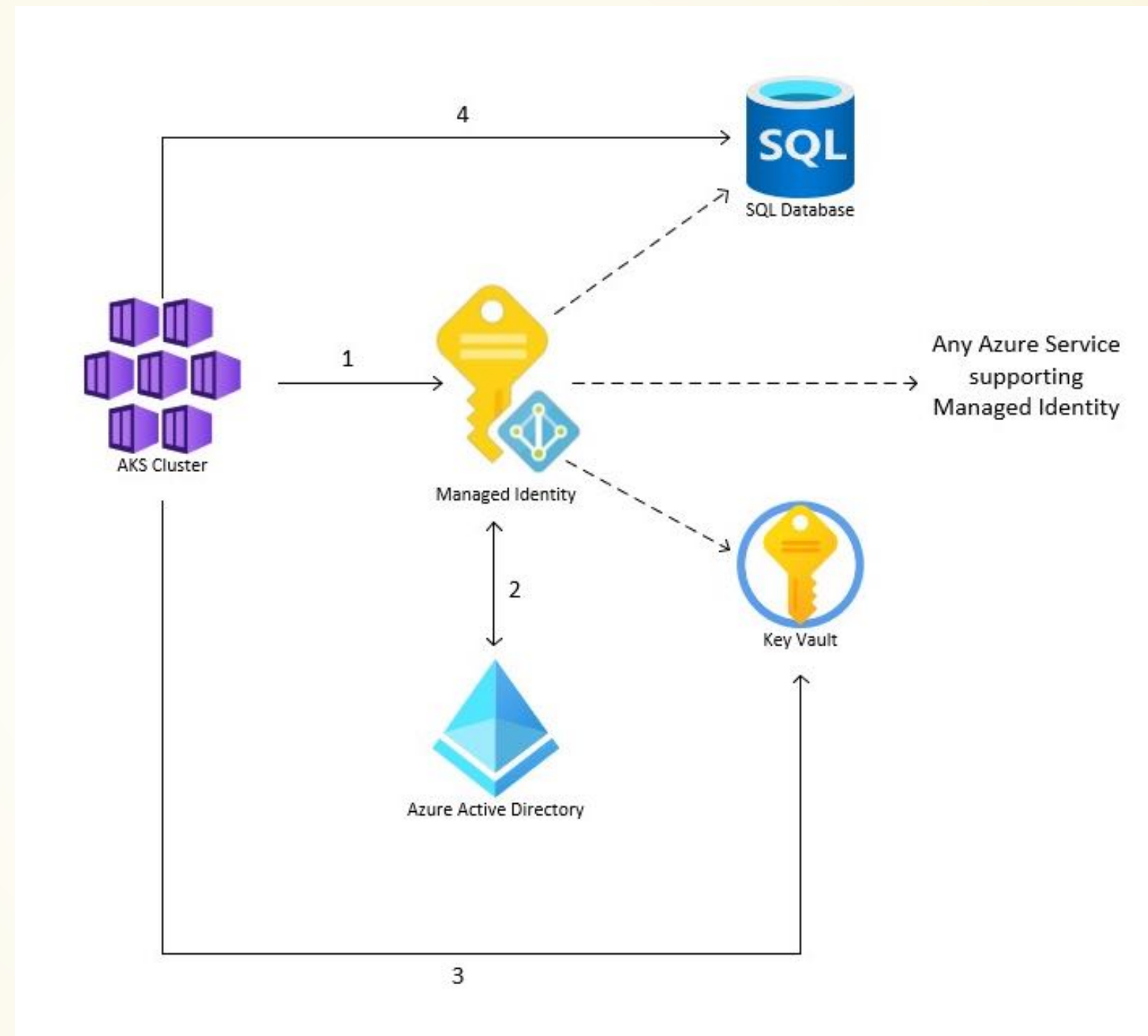


Role-Based Azure DevOps Repos + CI/CD Pipelines + Boards

The screenshot shows the Azure DevOps interface for a project named 'Caloudi NG'. The top navigation bar includes the Azure DevOps logo, the project name 'Caloudi NG', and a breadcrumb trail: 'Caloudi / Caloudi NG / Overview / Summary'. A search bar and user profile 'KS' are also visible. The left sidebar contains navigation options: Overview, Summary (selected), Dashboards, Wiki, Boards, Repos, Pipelines, Test Plans, and Artifacts. The main content area is titled 'Caloudi NG' and is marked as 'Private'. It features three main sections: 'About this project' with a description 'Angular client for Caloudi CSP and CMP platforms' and supported languages (CSS, TypeScript, HTML); 'Project stats' for the last 7 days, showing 0 work items created/completed, 0 pull requests opened, and 4 commits by 2 authors; and 'Members' with 8 team members represented by colored avatars (MS, ZH, CS, HT, KS, WL, JC, SH). At the bottom left, there is a 'Project settings' link.

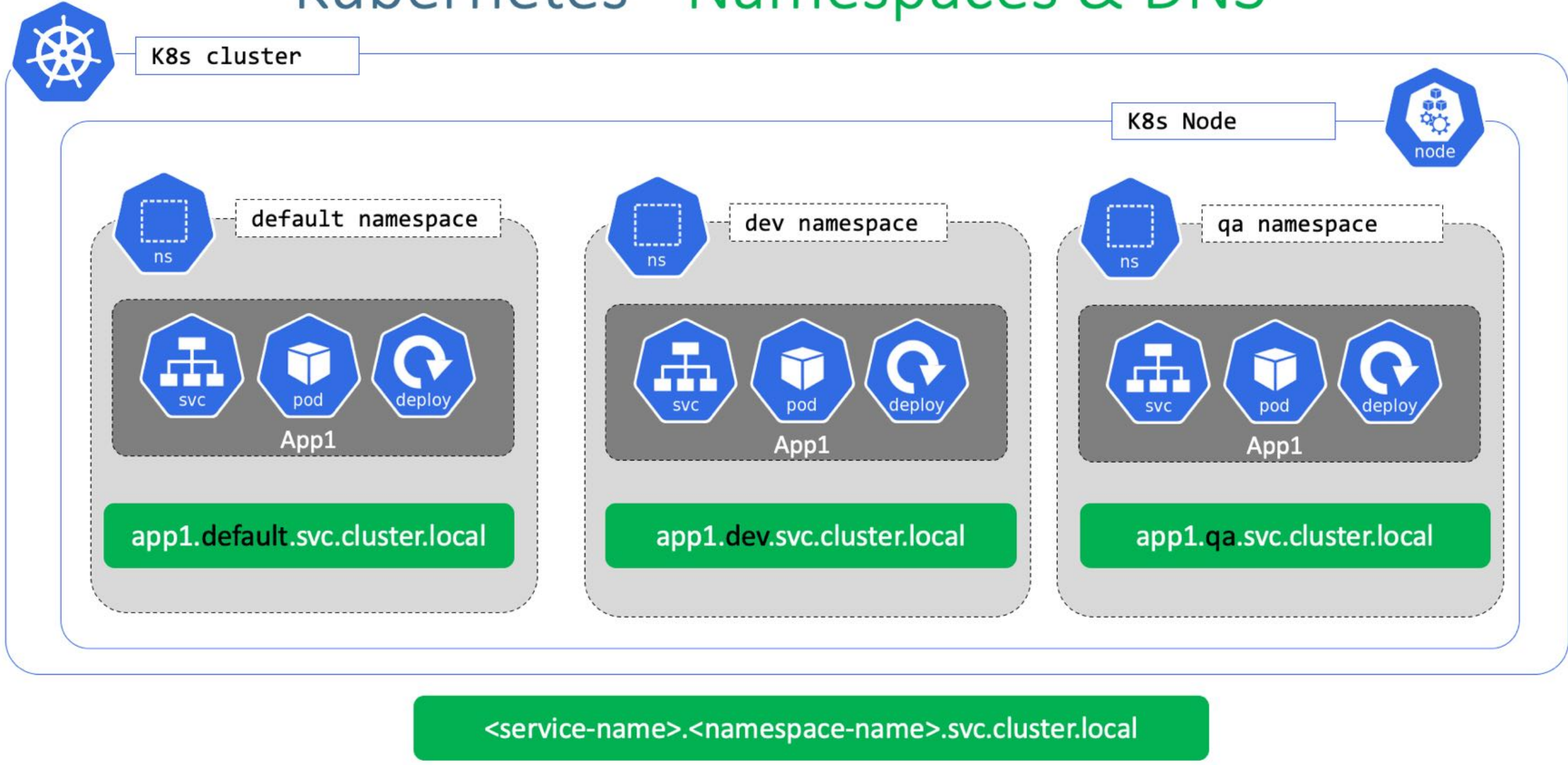
Azure Key Vault

- Security Credentials
- Connection Strings
- Configurations
- ...

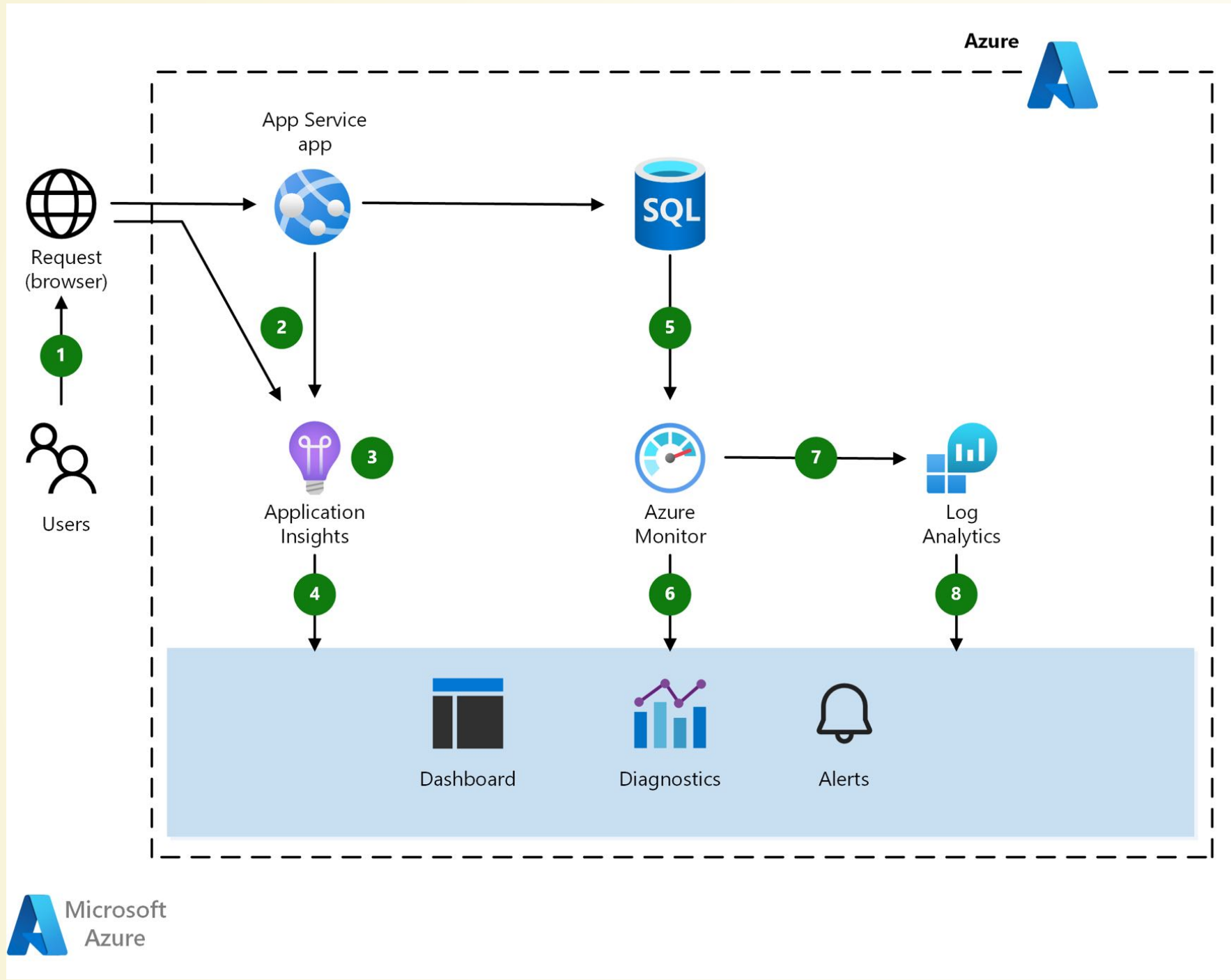


Azure Kubernetes Service

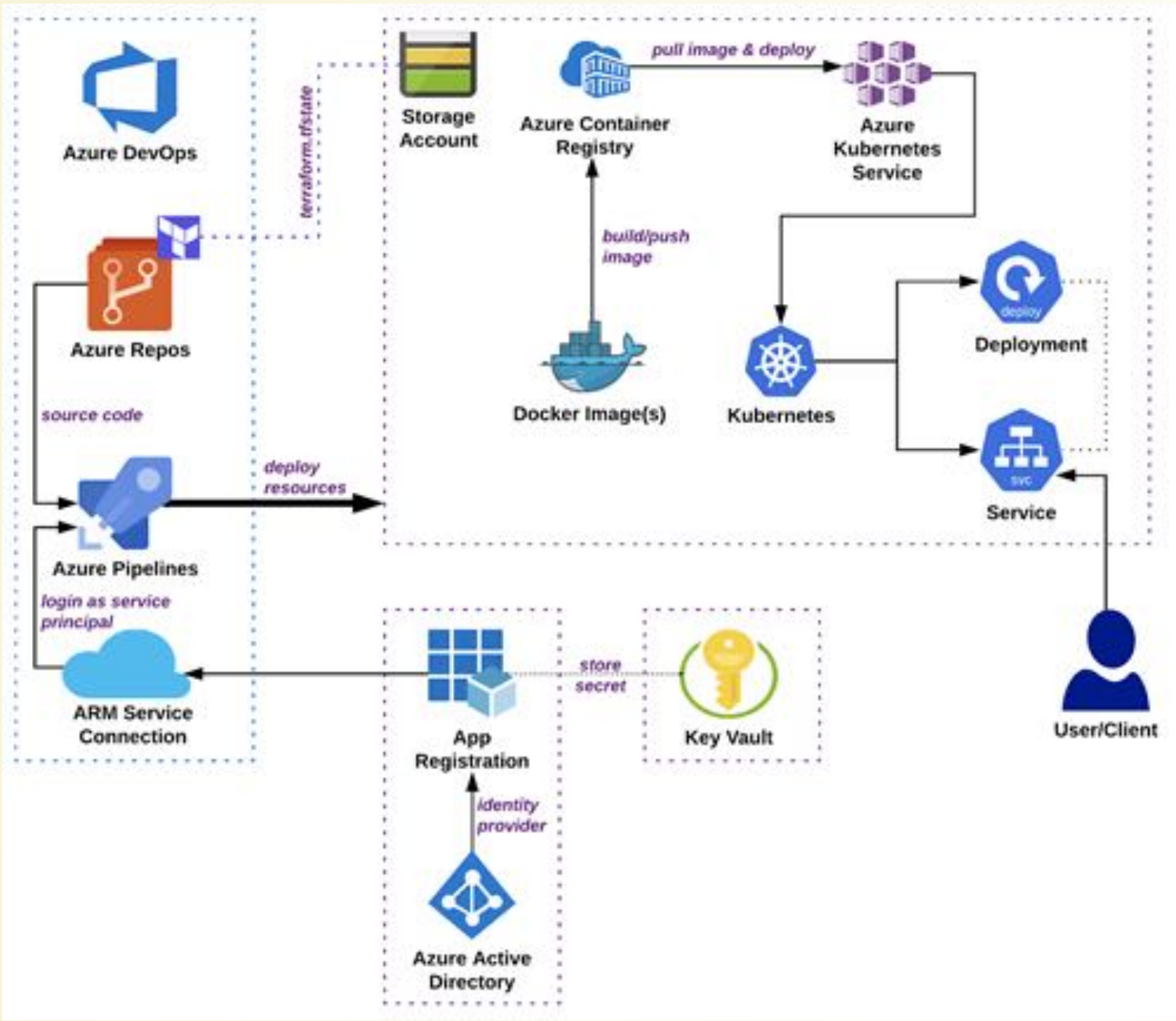
Kubernetes - Namespaces & DNS



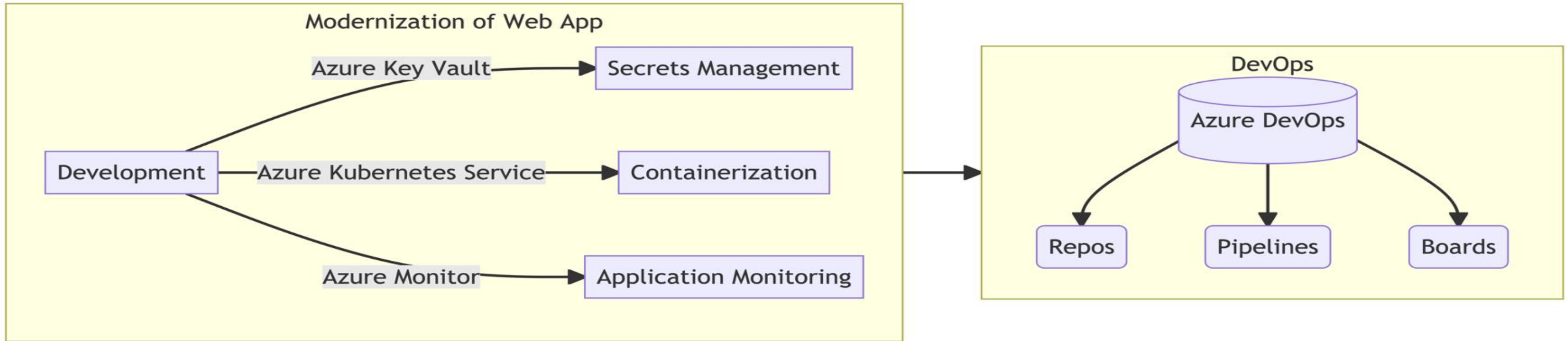
Azure Monitor



Typical Cloud Native Architecture



Dev -> Modernization -> DevOps



Trigger #2

ISO 27001

Scope = Infrastructure + Development + Product





Certificat
Certificate



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

敬啟 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√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

Tommy H.T. Dig

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 :

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) **2021-09-11** until **2024-09-10**
Ce certificat est valable à compter du (année/mois/jour) **2021-09-11** jusqu'au **2024-09-10**



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





The electronic certificate only, available at www.afnor.org, attests to real facts that the company is certified. Double-check the information, especially the number of the certificate. Répertoire COFRAC accessible sur www.cofrac.fr. Association COFRAC-AFNOR, Certification de Systèmes de Management. Points d'accès sur www.afnor.org. AFNOR is a registered trademark. AFNOR est une marque déposée. CERTIF 0003 - 04 000000

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 90 00 - F. +33 (0)1 48 17 90 00
SAS au capital de 10 187 000 € - 479 076 022 RCS Bobigny - www.afnor.org



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

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...



Source Code Analysis

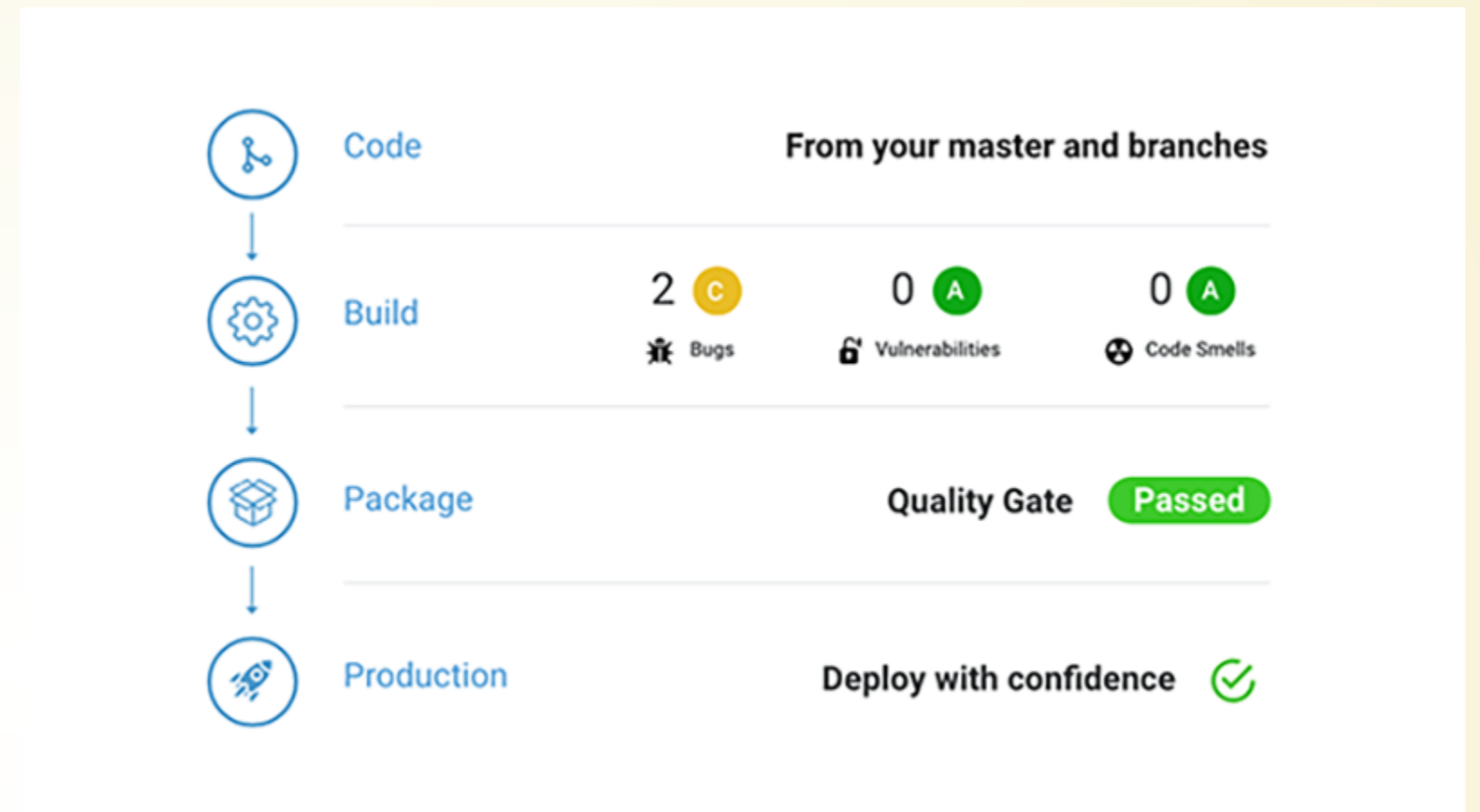
Static Analysis

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

Dynamic Analysis

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

Azure Devops 可以整合 SonarQube。



Software Composition Analysis

Code Analysis of

- Open Source Component
- 3rd-Party Library

For

- Vulnerability
- Outdated Component
- License Issue

The screenshot displays the Mend Bolt interface for a project named 'TestProject-CI (1)'. The main section is titled 'Open source risk report' and shows 'Total libraries: 430'. A summary card indicates a 'High' vulnerability risk with 10 vulnerable libraries. A severity distribution chart shows 7 High, 4 Medium, and 1 Low severity vulnerabilities. Below this, a table lists 12 security vulnerabilities under the 'Security vulnerabilities (12)' tab.

Severity	Vulnerability	Date	Library	Top Fix
H 9.1	CVE-2020-12265	04/26/2020	decompress-4.2.0.tgz	Upgrade to version 4.2.1 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12265
H 9.8	CVE-2019-10744	07/26/2019	lodash-4.17.11.tgz	Upgrade to version 4.17.12 https://github.com/lodash/lodash/pull/4336/commits/a01e4fa727e7294cb7b2645570ba96b206926790
H 9.8	CVE-2019-10746	08/23/2019	mix-in-deep-1.3.1.tgz	Upgrade to version 1.3.2.2.0.1 https://github.com/jonschlinkert/mix-in-deep/commit/8f464c8ce9761a8c9c2b3457eae9e9d404fa7a9
H 9.8	CVE-2019-10747	08/23/2019	set-value-2.0.0.tgz	Upgrade to version 2.0.1.3.0.1 https://github.com/jonschlinkert/set-value/commit/95e9d9923f8a8b4a01da1ea138fcc39ec7b6b15f
H 7.5	WS-2020-0044	03/08/2020	decompress-4.2.0.tgz	No fix available
H 9.8	CVE-2019-10747	08/23/2019	set-value-0.4.3.tgz	Upgrade to version 2.0.1.3.0.1 https://github.com/jonschlinkert/set-value/commit/95e9d9923f8a8b4a01da1ea138fcc39ec7b6b15f
M 5.6	CVE-2020-7598	03/11/2020	minimist-0.0.8.tgz	Upgrade to version minimist - 0.2.1.1.2.3

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

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。

The screenshot displays the 'Tests' tab in Azure DevOps for a 'WhiteSource Bolt Build Report'. The summary shows 1 run completed with 0 passed and 1 failed, resulting in 3 unique failing tests. A donut chart indicates 0 passed, 3 failed, and 0 other tests. The test results table lists the following tests:

Test	Duration	Failing since	Failing build
× NUnit Test Run (3/3)	0:00:13.520		
× Web Browser XSS	0:00:00.000	Just now	20190812.5
× X-Content-Type-O	0:00:00.000	Just now	Current bu
× X-Frame-Options	0:00:00.000	Just now	Current bu

The detailed view for the 'Web Browser XSS Protection Not Enabled' test shows the following error message and stack trace:

```
<p>Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-Content-Type-Options' header.</p>
```

Solution:
<p>Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP header to 1. For more information, see the following Reference:</p>

Reference:
<p>[https://www.owasp.org/index.php/XSS_\(Cross_Site_Scripting\)_Prevention_Cheat_Sheet](https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet)</p><p>Instances of the error:</p>

- * http://172.17.0.1:5000/ - GET
- * http://172.17.0.1:5000/sitemap.xml - GET
- * http://172.17.0.1:5000 - GET
- * http://172.17.0.1:5000/robots.txt - GET

參考資料：OWASP/ZAP Scanning extension for Azure DevOps

參考資料：Running OWASP ZAP in Azure Kubernetes Service

The image shows a screenshot of the Azure DevOps web interface. The top navigation bar includes 'Azure DevOps', 'Caloudi', 'Caloudi NG', 'Repos', and 'Files'. A search bar is located on the right. The left sidebar contains navigation options: Overview, Boards, Repos, Files, Commits, Pushes, Branches, Tags, Pull requests, Pipelines, Test Plans, and Artifacts. The main area displays the file 'azure-pipelines.cmp-ng.sonarqube.yml' in the 'develop' branch. The file content is as follows:

```
20 - task: SonarQubePrepare@5
21   displayName: Preparing Sonar
22   inputs:
23     SonarQube: ' -sonarqube-service-connection-Caloudi NG'
24     scannerMode: 'CLI'
25     configMode: 'manual'
26     cliProjectKey:
27     cliProjectName:
28     #cliSources: './src'
29     extraProperties: |
30       # Additional properties that will be passed to the scanner,
31       # Put one key=value per line, example:
32       sonar.host.url=http://.cloudapp.azure.com:9000
33       sonar.ws.timeout=120
34       sonar.projectKey=
35       sonar.projectName=
36       sonar.language=ts
37       sonar.sourceEncoding=UTF-8
38       sonar.sources=src
39       sonar.typescript.tsconfigPath=tsconfig/tsconfig.sonar.json
40       sonar.exclusions=**/node_modules/**,**/*.css,**/*.html
41
42 # Run Code Analysis task
43 - task: SonarQubeAnalyze@5
44   displayName: SonarQube Co
45
46 # Publish Quality Gate Resu
47 - task: SonarQubePublish@5
48   # timeoutInMinutes: 2
49   inputs:
50     pollingTimeoutSec: '300'
```

The bottom right pane shows a pipeline run summary for '#20220711.6 • Merge branch 'develop' of https://dev.azure.com/Caloudi/Caloudi%20NG/_git/Caloudi.NG.C...'. The run is marked as 'Failed' and includes a 'SonarQube Analysis Report' section with the following details:

- Caloudi CMP NG Quality Gate: **Failed**
- Reliability Rating on New Code: **E** > A
- Detailed SonarQube report > [link](#)

Vulnerability Scan Report

Perspective: Overall Status | Sort by: Name | Search by project name or key | 4 projects

★ **Caloudi CMP API** Failed | Last analysis: 11 days ago

Bugs	Vulnerabilities	Hotspots Reviewed	Code Smells	Coverage	Duplications	Lines
14 C	5 D	0.2% E	2.8k A	0.0% F	19.2% C	41k M C#

☆ **Caloudi CMP NG** Failed | Last analysis: 5 days

Bugs	Vulnerabilities	Hotspots Reviewed	Code Smells	Coverage	Duplications
43 D	0 A	0.0% E	328 A	0.0% F	12.7%

Perspective: Overall Status | Sort by: Name | Search by project name or key | 4 projects

☆ **Caloudi CMP NG** Passed | Last analysis: yesterday

Bugs	Vulnerabilities	Hotspots Reviewed	Code Smells	Coverage	Duplications	Lines
0 A	0 A	100% A	2.8k A	-	0.0% F	42k M C#

☆ **Caloudi CSP API** Failed | Last analysis: 21 days

Bugs	Vulnerabilities	Hotspots Reviewed	Code Smells	Coverage	Duplications
1 C	4 D	1.3% E	1.9k A	0.0% F	27.1%

☆ **Caloudi CMP NG** Passed | Last analysis: yesterday

Bugs	Vulnerabilities	Hotspots Reviewed	Code Smells	Coverage	Duplications	Lines
0 A	0 A	100% A	328 A	-	0.0% F	66k M TypeScript

☆ **Caloudi GCP API** Failed | Last analysis: 2 months

Bugs	Vulnerabilities	Hotspots Reviewed	Code Smells	Coverage	Duplications
24 C	6 D	0.0% E	3.3k A	0.0% F	21.9%

☆ **Caloudi CSP API** Passed | Last analysis: 23 hours ago

Bugs	Vulnerabilities	Hotspots Reviewed	Code Smells	Coverage	Duplications	Lines
0 A	0 A	100% A	1.9k A	-	0.0% F	27k M C#

☆ **Caloudi GCP API** Passed | Last analysis: 2 hours ago

Bugs	Vulnerabilities	Hotspots Reviewed	Code Smells	Coverage	Duplications	Lines
0 A	0 A	100% A	3.5k A	-	0.0% F	50k M C#

WhiteSource Bolt

文件名稱: 弱點處理報告單
文件編號: C-1-B-08-02 版本: 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		掃描時間	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	<input checked="" type="checkbox"/> 已修補 <input type="checkbox"/> 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	<input type="checkbox"/> 已修補 <input checked="" type="checkbox"/> 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。
			<input type="checkbox"/> 已修補 <input type="checkbox"/> 暫不修補		
			<input type="checkbox"/> 已修補 <input type="checkbox"/> 暫不修補		
			<input type="checkbox"/> 已修補 <input type="checkbox"/> 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

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-cmhc-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

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-cmhc-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

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

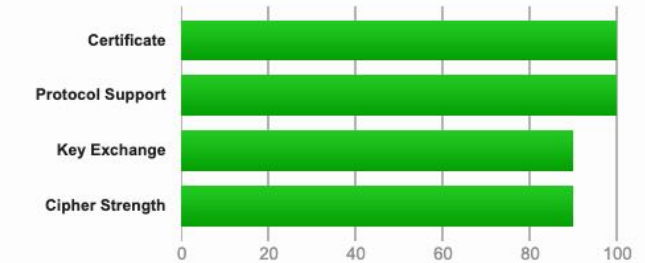
You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > crp.8isoft.com

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

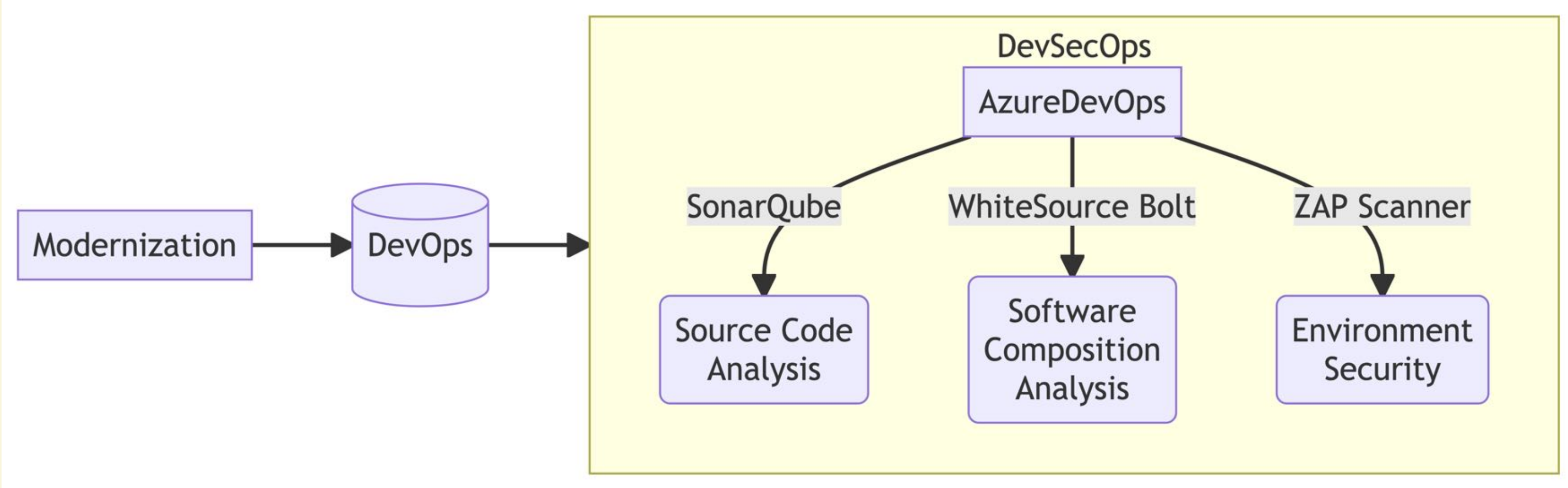
Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

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





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 :

Certificat
Certificate



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

<p>敬啟 公司/單位名稱：卡洛地股份有限公司</p> <p>管理代表/負責人：[redacted] 先生</p> <p>審查結果： 貴公司於 <u>2022-07-11</u></p> <p>執行 <u>NF EN ISO/IEC 27001:2017(Europe)-ISO/IEC 27001:2013+COR 1:2014+COR 2:2015 (International)</u> 驗證審查， 經艾法諾集團 驗證經理審查結果如下：(打√者)</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> 矯正措施符合驗證標準要求。 <input type="checkbox"/> 現場稽核未發現不符合項目。 經驗證決定小組核定： <input type="checkbox"/> 予以發證。 <input checked="" type="checkbox"/> 此次驗證通過，證書持續有效。 <input type="checkbox"/> 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。

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



CERTIFICATION DE SYSTEMES DE MANAGEMENT
ACCREDITATION AF 42021
RECOGNISEE PAR WWW.COFRAC.FR



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



The electronic certificate only, available at www.afnor.org, attests to real-time that the company is certified. Double-check the electronic certificate on our website. www.afnor.org. NF is an acronym for the certification of systems. COFRAC accreditation n°42021, Management Systems Certification. Registre available at www.afnor.org. Association COFRAC AFNOR, Certification de Systèmes de Management. Points d'accès sur www.afnor.org. AFNOR is a registered trademark. AFNOR est une marque déposée. CERTIF 0003 - 04 100000

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 90 00 - F. +33 (0)1 48 17 90 00
SAS au capital de 10 187 000 € - 479 076 002 RCS Bobigny - www.afnor.org



貝爾國際驗證機構
系統管理部



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

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...



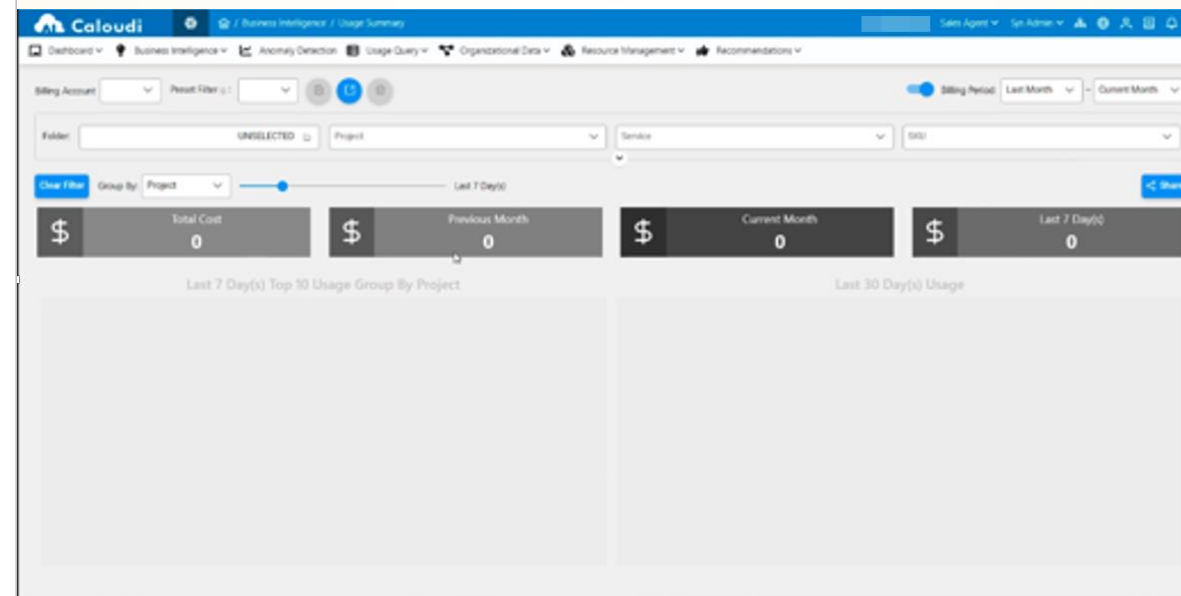
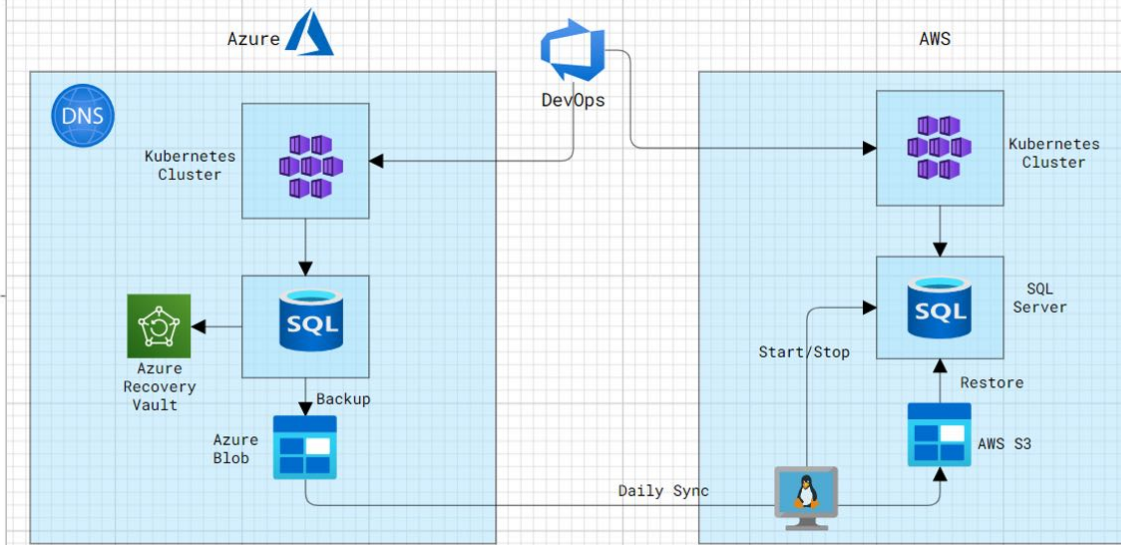
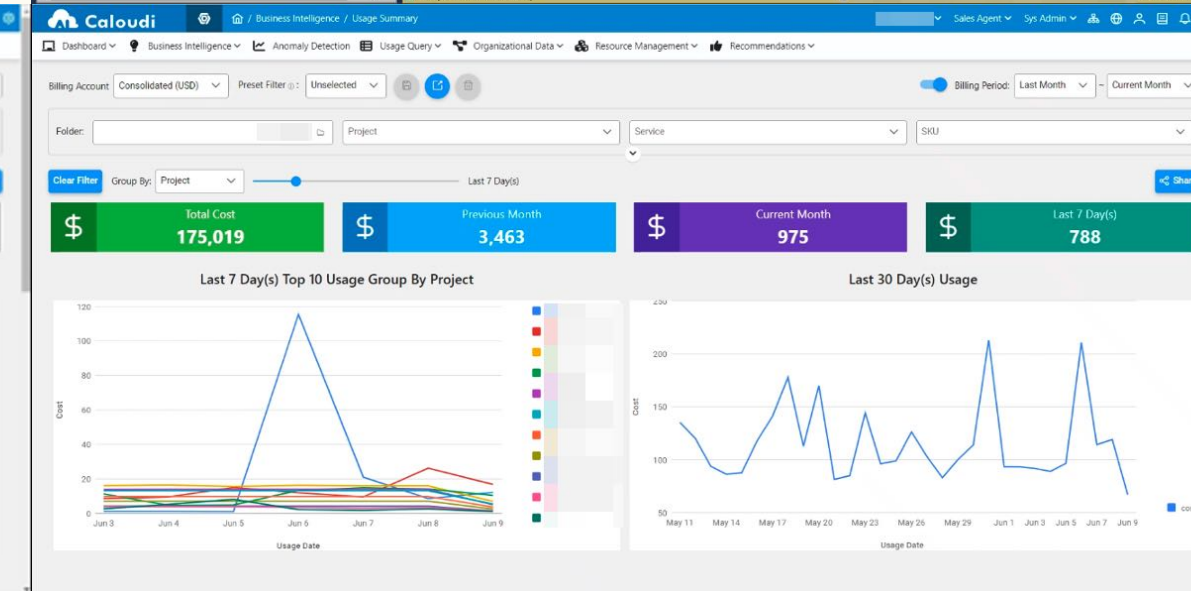

Disaster Recovery

文件名稱：業務持續運作計畫演練活動紀錄
文件編號：C-I-B-14-03


版次：1.0

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
規劃執行日期	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	權責單位主管	

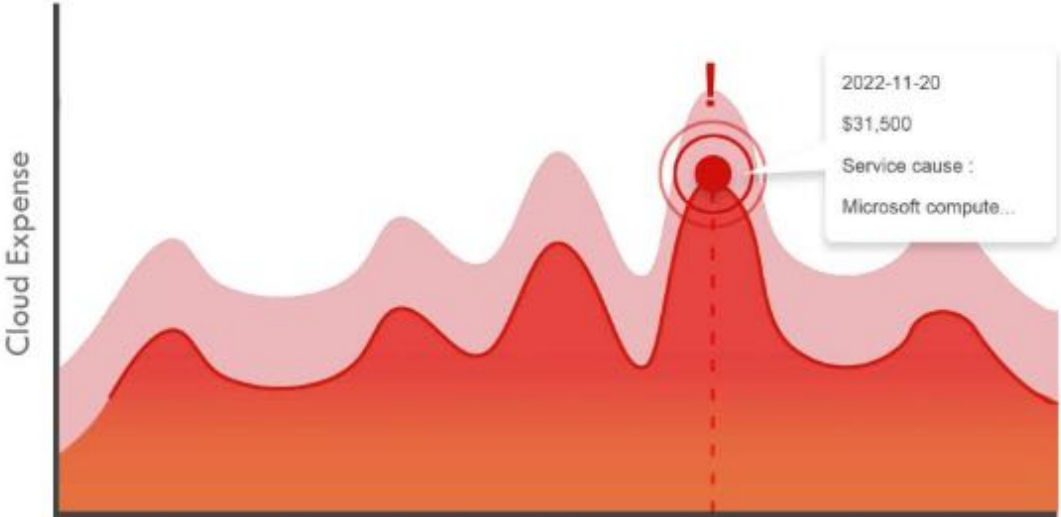
雲端費用 Anomaly Detection

Pricing Contact Us English ▾CRP Login

Resource Monitoring and Planning

AI MonitorAllocation RecommendationBudgeting

8iSoft DL Model
Dev-AnomalyProj



Cloud Expense

Date 01/05 01/07 01/09 01/15 01/21 01/24 01/30

2022-11-20
\$31,500
Service cause :
Microsoft compute...

The chart displays cloud expense over time, with a significant spike on 2022-11-20. The spike is highlighted with a red circle and a red exclamation mark, indicating an anomaly. The expense for that day is \$31,500. The service cause is identified as 'Microsoft compute...'. The chart also shows a secondary, lower-level spike around 01/15.

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

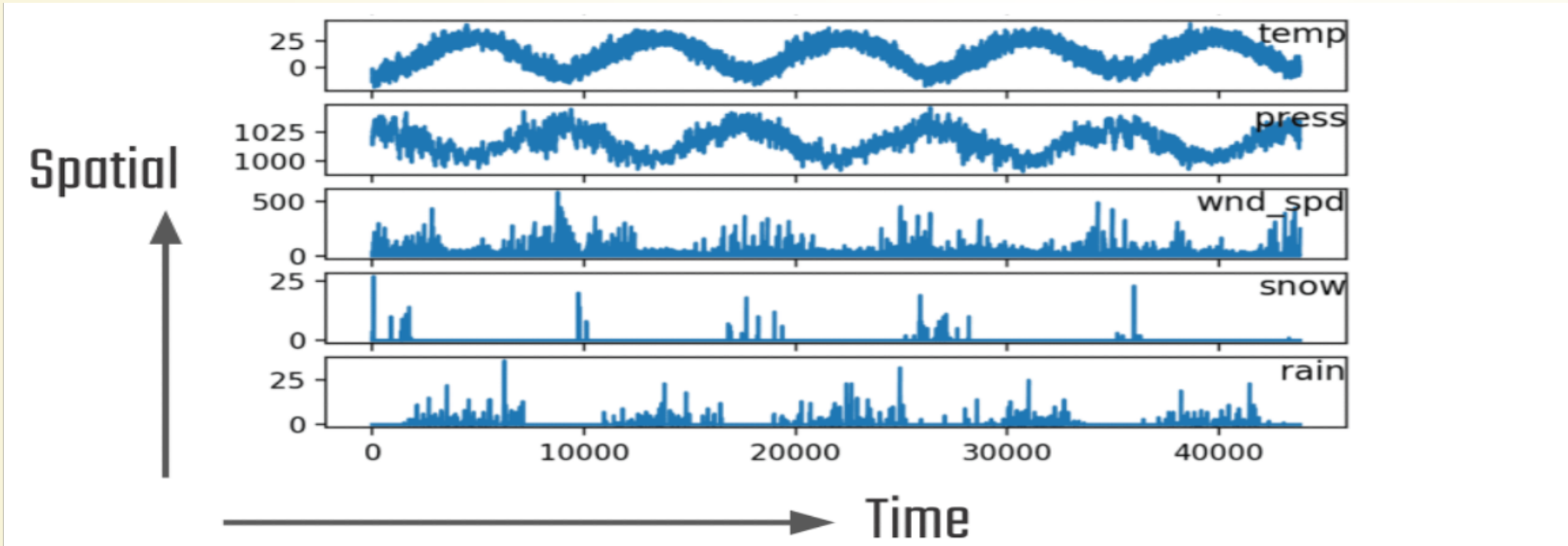
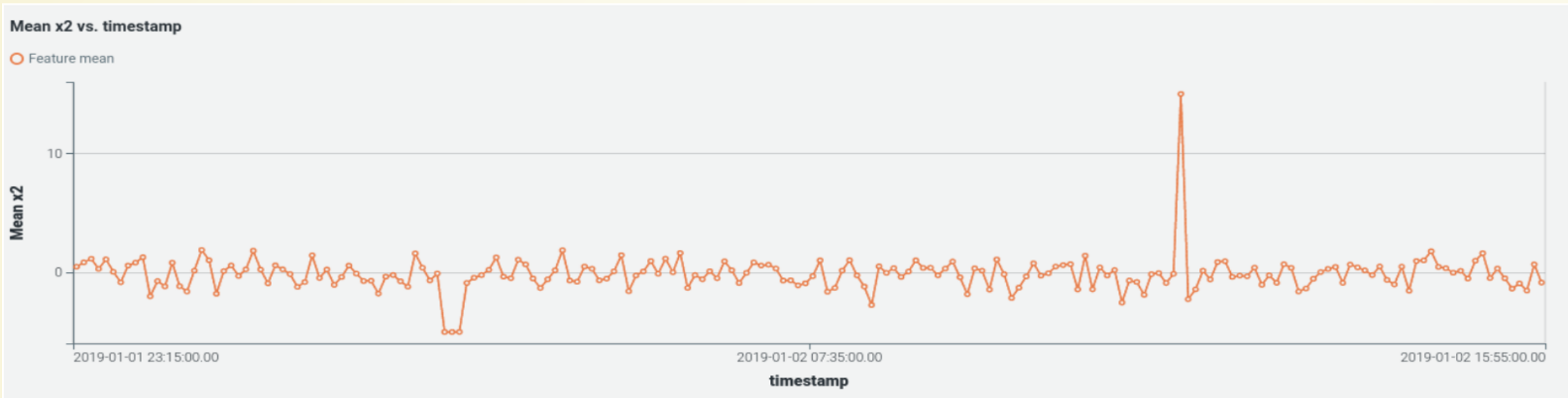
Billing Data / Log Data 都是 Time-Series Data

The screenshot displays the Microsoft Azure Cost Management interface. On the left, a bar chart shows 'Accumulated costs' for October 2019. The chart includes a legend with categories: Daily cost (green), Est daily budget (red), Overage (red), Forecast cost (light green), and Overage forecast (pink). A red box highlights the 'Granularity: Daily' dropdown menu. The right pane shows the 'All resources' view for 'Caloudi Corporation', with filters for 'Log', 'Subscription equals all', 'Resource group equals all', 'Type equals all', and 'Location equals all'. Below the filters, there are summary cards for '3 Unsecure resources' and '0 Recommendations'. A table lists resources with checkboxes, names, and types.

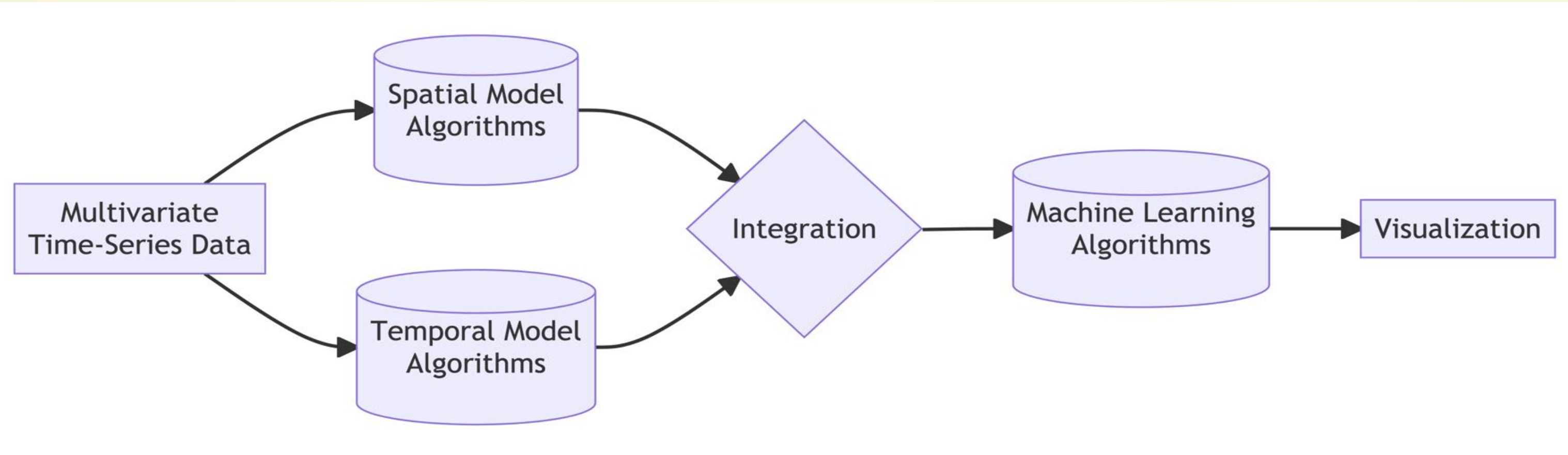
Name	Type
-k8s-log	Log Analytics workspace
ContainerInsights(-k8s-log)	Solution

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

The screenshot shows a web application interface for a cloud resource health check. At the top center is a logo consisting of a cloud with a stylized 'A' inside. Below the logo is the title "Cloud Resource Usage Health Check" and a small footer "Caloud | Version:1.0.0 | Contact:zxc@gmail.com".

The main interface features a file upload section with the text "Choose a Raw File:". Below this is a teal-colored area with the text "Drag and drop file here" and "Limit 200MB per file + CSV". A "Browse files" button is located on the right side of this area. Below the teal area, a file named "machine-2-7.csv" with a size of "8.1MB" is listed. A "Calculate" button is positioned below the file list.

At the bottom of the interface is a chart titled "Multivariate Time Series Anomaly Detection". The chart displays two data series, labeled "1" and "2", on a grid. The y-axis ranges from -0.5 to 0.5. Red vertical bars of varying heights indicate detected anomalies in the data series.

Multivariate Time-Series Data Anomaly Detection via Graph Attention Network

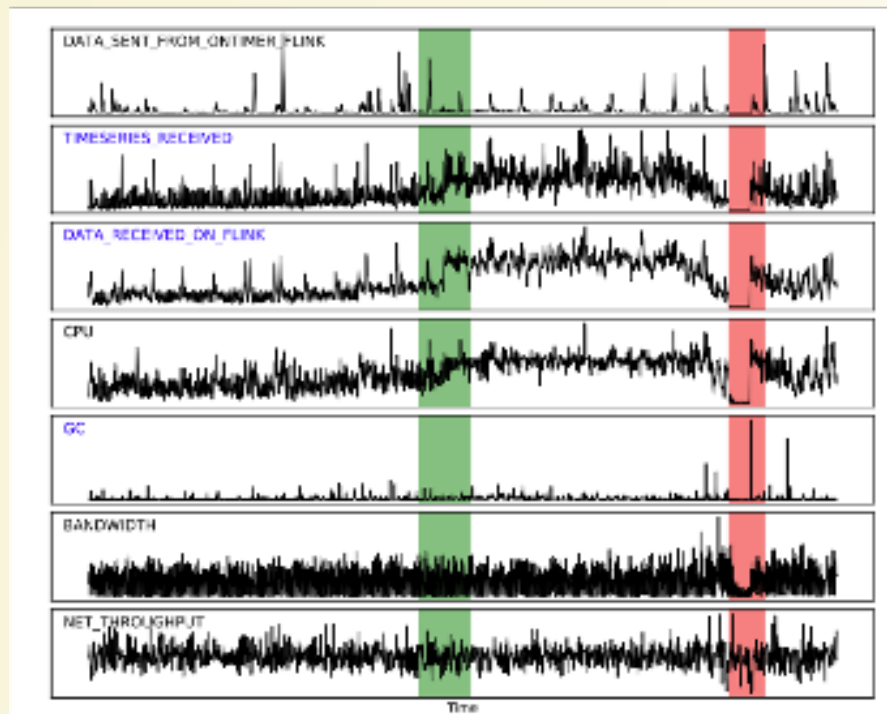


Fig. 1. An example of multivariate time-series input. Green indicates normal values and red indicates anomalies.

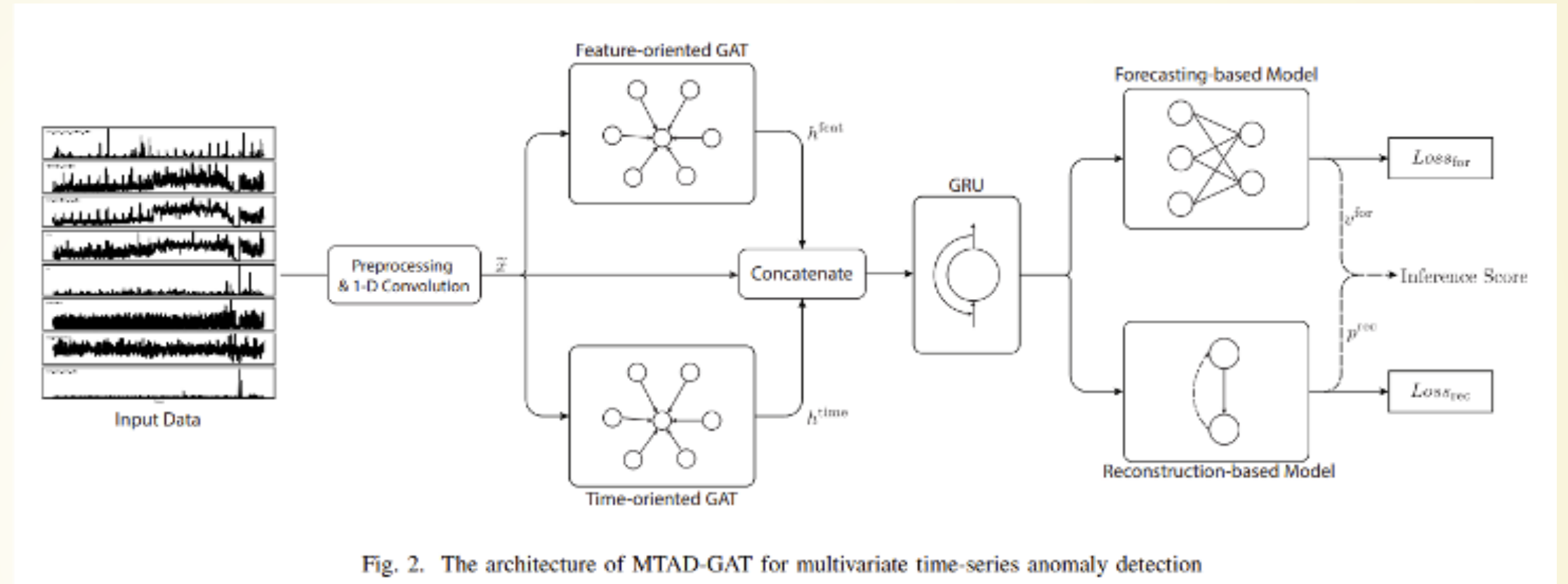
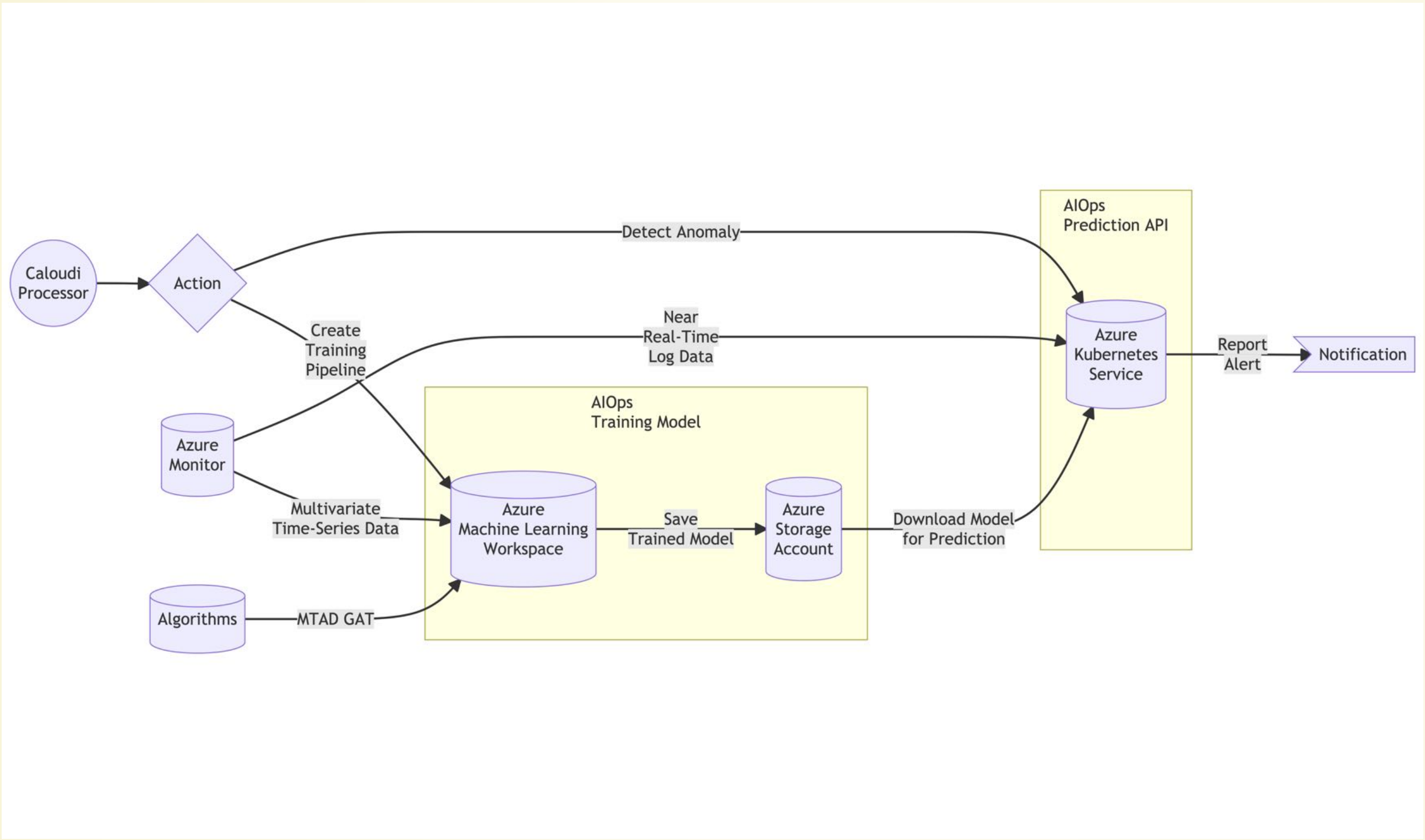


Fig. 2. The architecture of MTAD-GAT for multivariate time-series anomaly detection

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 }]]

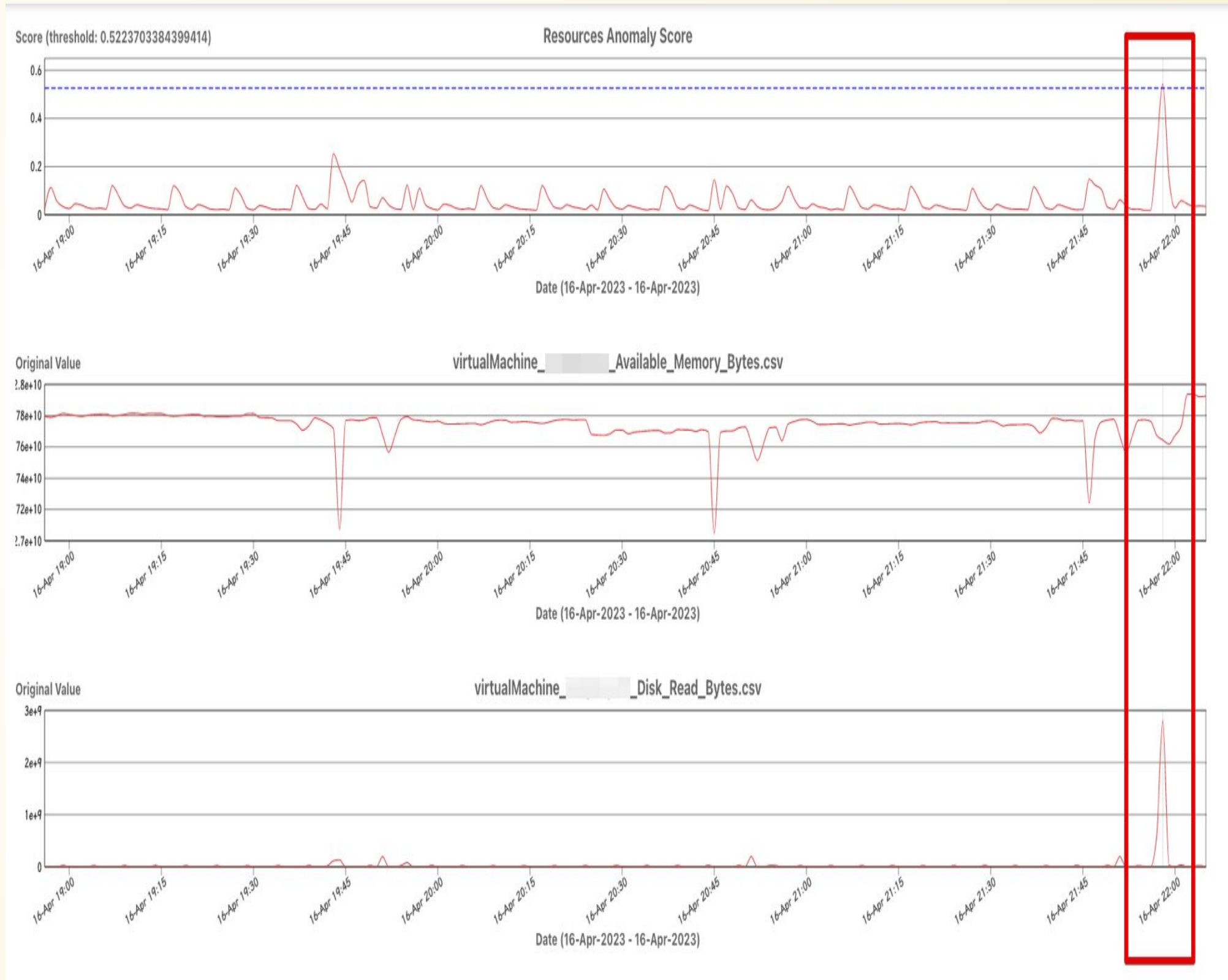
Anomaly Time : ["04/16/2023 21:58:00"]

Stamps :

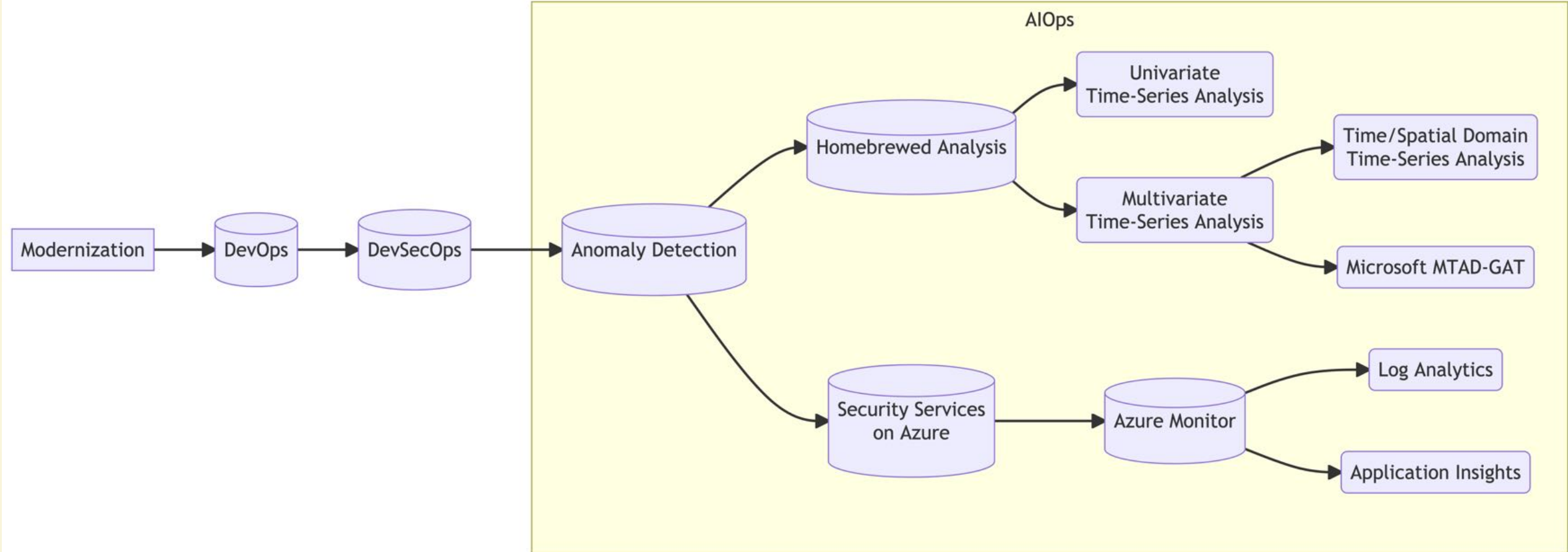
[View Report](#)

Sent by Cloud Resource Planning Platform

If you have any questions, please send to [support](#).



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

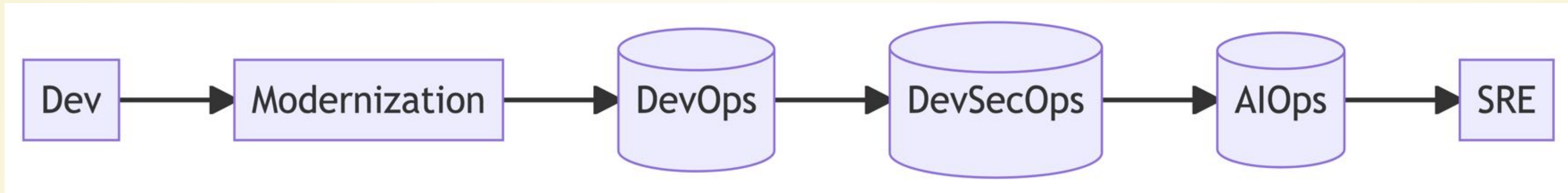


Why AIOps

- 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。

