

AWS 雲端資訊安全說明



AWS雲端專案 - 大綱

目的

- 1.在 SIEM 部屬前的暫時替代方案
- 2.透過自製工具，協助管理員發現異動，並主動推至 Teams 通知

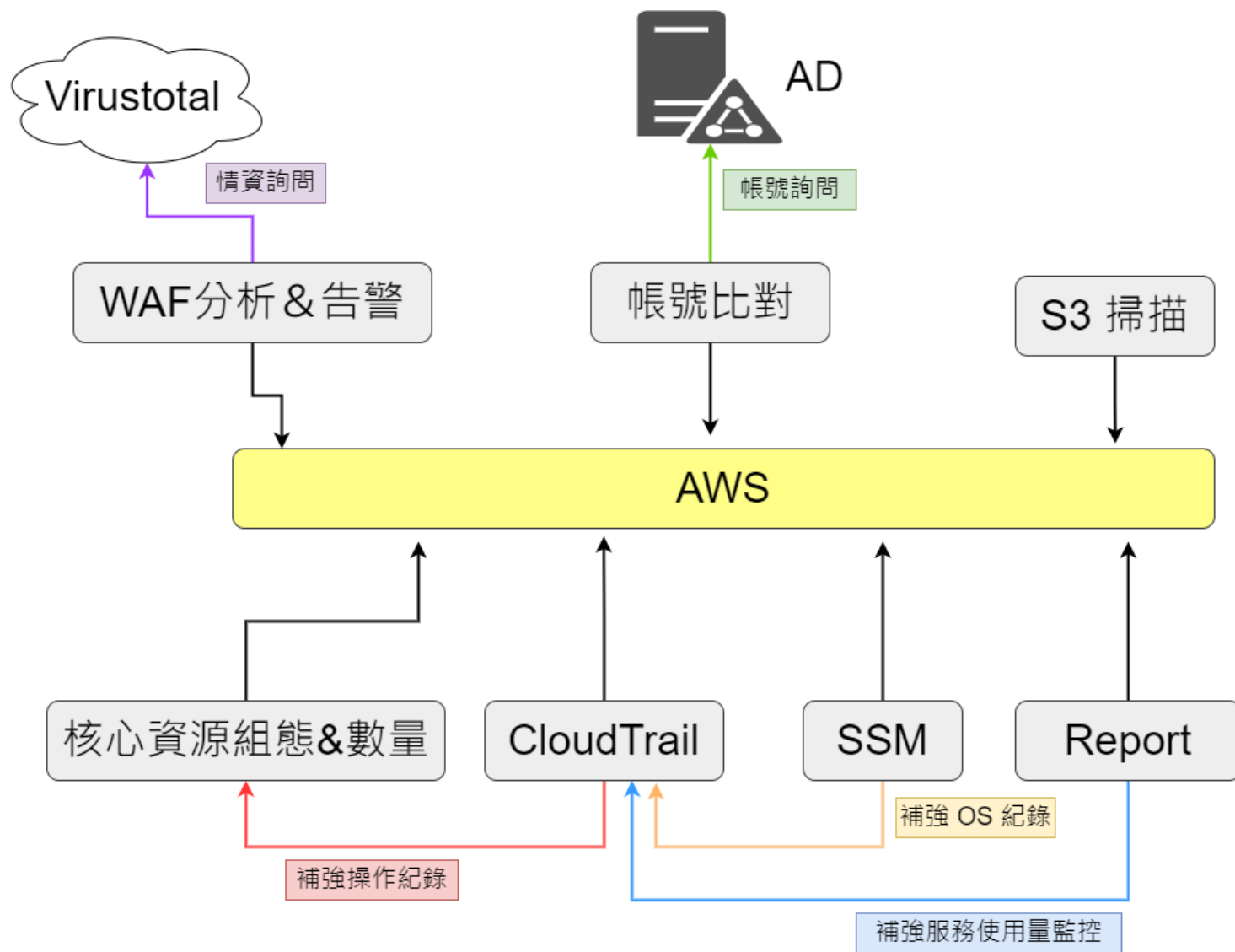
未來

- 1.在 SIEM 部屬後，仍可作為 Log 分析工具
- 2.客製化告警，可更貼近公司文化 (ex.離職帳號刪除)

成效

- 1.於資源異動時，可以快速被告知
- 2.結合 VirusTotal 獲得情資，早一步分析情況
- 3.透過 Log 彙整，可得知是否有非預期的異常的行為

AWS雲端專案 - 資訊安全示意圖 v0.1



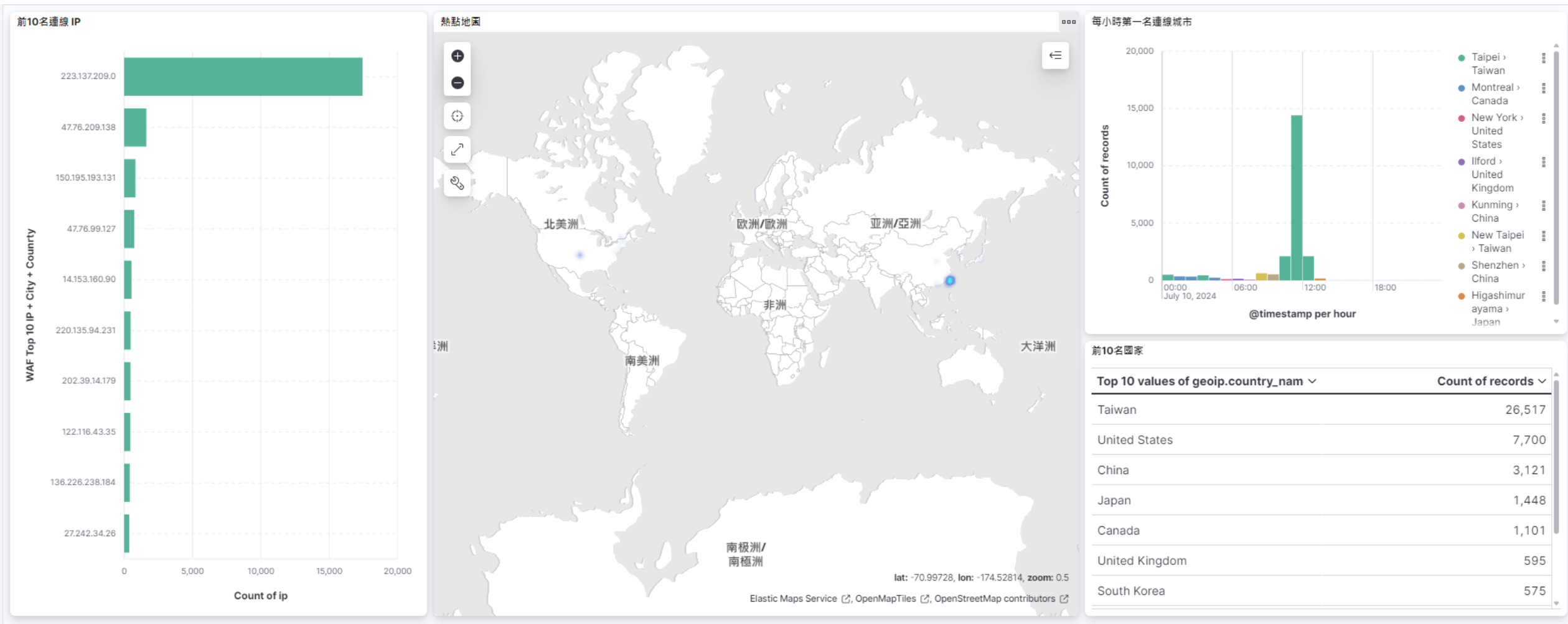
AWS雲端專案 – 外部防禦策略



透過 WAF 的成效觀察與外部掃描 S3
，帳號管理等方式

來防範網路的攻擊與資料的外洩

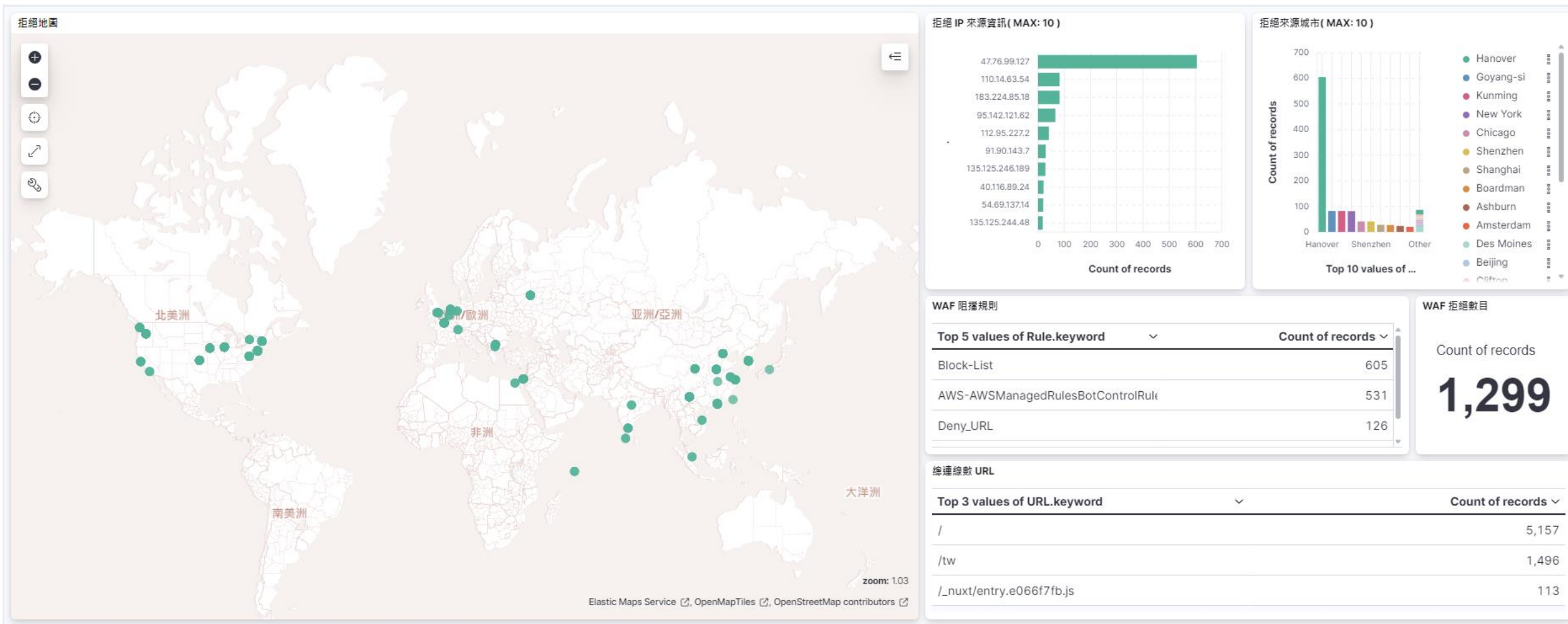
AWS雲端專案 – 來源熱點地圖



目的：提供資安判定防禦策略(ex.拒絕國家連線)

功能：直觀提供官網總連線區域地圖與數量

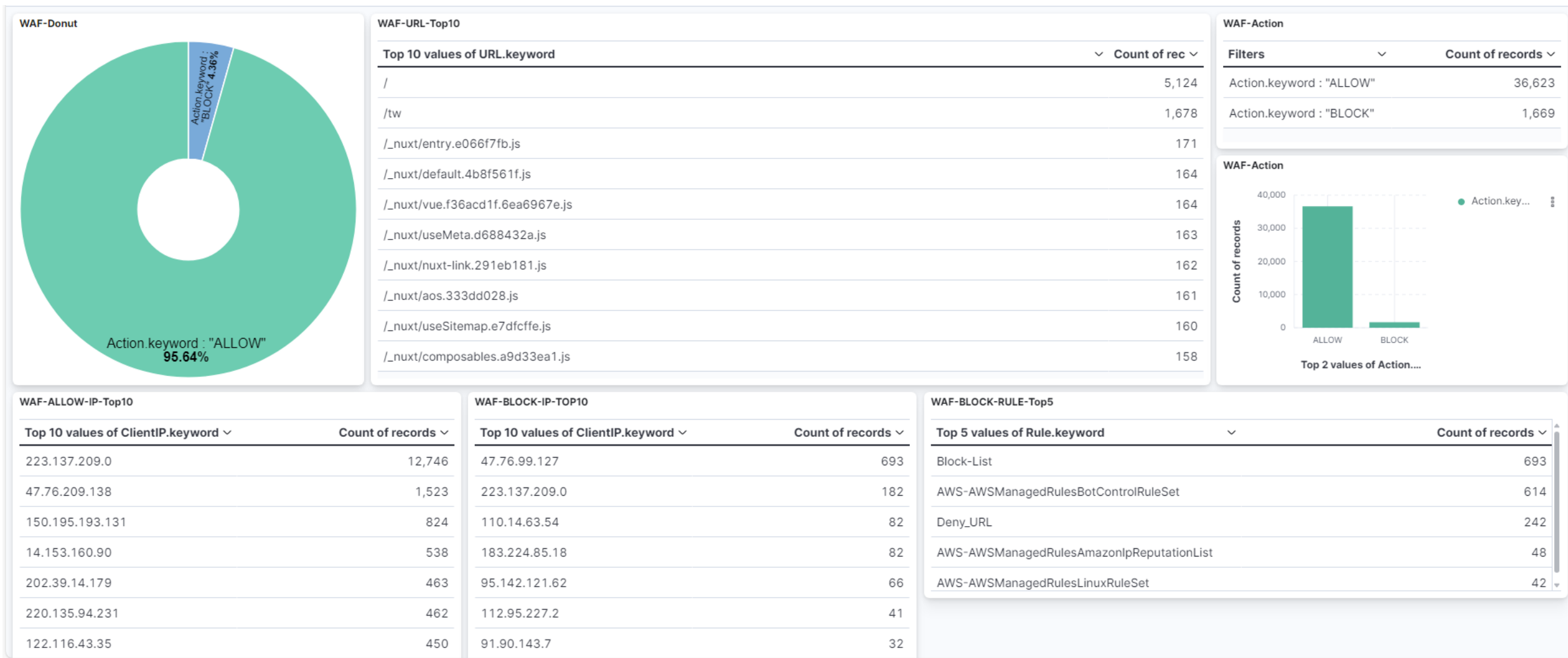
AWS雲端專案 – WAF 阻擋熱點地圖



目的：提供資安判定防禦策略(ex.拒絕國家連線)

功能：直觀提供 WAF 阻擋區域地圖與數量

AWS雲端專案 – WAF 可視化 Dashboard



目的：WAF 防禦成效分析

功能：TOP 10 允許IP & 拒絕 IP，與拒絕原因總覽

AWS雲端專案 – Team主動推送（WAF防禦）

定時掃描結果概覽

VirusTotal 每小時 Action:ALLOW - Top10 檢查

告警等級：正常 

IP地址: 136.226.229.16 數量: 579 是否惡意: False 發現的引擎數量: 0
IP地址: 120.219.57.103 數量: 305 是否惡意: False 發現的引擎數量: 0
IP地址: 45.76.122.71 數量: 125 是否惡意: True 發現的引擎數量: 2
IP地址: 45.76.44.221 數量: 119 是否惡意: True 發現的引擎數量: 4
IP地址: 103.14.141.200 數量: 113 是否惡意: False 發現的引擎數量: 0
IP地址: 141.164.48.161 數量: 112 是否惡意: False 發現的引擎數量: 0
IP地址: 167.172.175.168 數量: 108 是否惡意: False 發現的引擎數量: 0
IP地址: 209.97.171.44 數量: 105 是否惡意: False 發現的引擎數量: 0
IP地址: 101.9.194.67 數量: 100 是否惡意: False 發現的引擎數量: 0
IP地址: 165.22.122.238 數量: 85 是否惡意: True 發現的引擎數量: 1

目的：WAF 放行的 IP , 再次確認安全性

功能：通過的 TOP-10 IP 傳送至 Virustotal 情資檢查

定時掃描結果概覽

VirusTotal 每小時 Action:ALLOW - Top10 檢查

告警等級：警告 

IP地址: 114.136.111.107 數量: 445 是否惡意: False 發現的引擎數量: 0
IP地址: 120.237.81.195 數量: 436 是否惡意: False 發現的引擎數量: 0
IP地址: 114.34.184.108 數量: 363 是否惡意: False 發現的引擎數量: 0
IP地址: 39.9.226.46 數量: 277 是否惡意: False 發現的引擎數量: 0
IP地址: 185.119.0.206 數量: 210 是否惡意: True 發現的引擎數量: 1
IP地址: 65.154.226.170 數量: 186 是否惡意: True 發現的引擎數量: 8
IP地址: 35.184.34.71 數量: 184 是否惡意: False 發現的引擎數量: 0
IP地址: 112.175.250.218 數量: 183 是否惡意: False 發現的引擎數量: 0
IP地址: 185.119.0.215 數量: 181 是否惡意: False 發現的引擎數量: 0
IP地址: 27.50.59.146 數量: 114 是否惡意: True 發現的引擎數量: 1

目的：訊息強調化，可快速訊息瀏覽

功能：若引擎數 >7, 數量 > 1000則紅字標示，並變更告警等級

AWS雲端專案 – Team主動推送 (WAF防禦)

查詢高風險 IP (引擎數 >7) 七天內出現數目

VirusTotal 高風險 IP 檢查

告警等級：分析     

高風險IP比對: 195.170.172.128

DATE:2024-11-23 ,出現條(小時/天)數 : 0, 連線總數 : 0

DATE:2024-11-22 ,出現條(小時/天)數 : 0, 連線總數 : 0

DATE:2024-11-21 ,出現條(小時/天)數 : 0, 連線總數 : 0

DATE:2024-11-20 ,出現條(小時/天)數 : 0, 連線總數 : 0

DATE:2024-11-19 ,出現條(小時/天)數 : 0, 連線總數 : 0

DATE:2024-11-18 ,出現條(小時/天)數 : 0, 連線總數 : 0

DATE:2024-11-17 ,出現條(小時/天)數 : 0, 連線總數 : 0


Important: You must update your Webhook URL for this connection in Teams. [Learn more about this update](#)

目的：自動歷史查詢七天內出現次數

功能：若引擎數 >7, 則將該 IP 自動反查七天內的歷史，協助管理員判定是否加入黑名單

WAF Block 行為告警 (15 分鐘內)

15分鐘內 AWS WAF 拒絕數量上限值

告警等級：警告     

目前數目：5171 > 警戒數目：200

目的：高拒絕數時，應主動介入查看狀態

功能：WAF 總阻擋數 > 200 告警

AWS雲端專案 – Team主動推送（ WAF防禦 ）

WAF ALLOW 行為告警 (15 分鐘內)

15分鐘內 AWS ALLOW 允許數量上限值

告警等級：警告 ⚡ ⚡ ⚡ ⚡ ⚡

目前數目：152 > 警戒數目：100

TOP 3 連線

IP: 49.234.3.160, 數目：101, 國家：China

IP: 85.193.0.175, 數目：45, 國家：Czechia


IP: 95.217.176.173, 數目：43, 國家：Finland

Important: You must update your Webhook URL for this connection in your Teams. [Learn more about this update](#)

目的：加強高連線時判斷

功能：加入 GeoIP 資料庫，自動判斷前 3 連線的 IP 來源國家，協助管理者判斷是否加入黑名單

AWS雲端專案 – Team主動推送（外部 S3 掃描）

 allen-test 下午 05:05

每日外部 S3 Bucket 掃描

搜尋關鍵字：hannstar

警告 ⚡ ⚡ ⚡ ⚡ ⚡

== LazyS3 ==

Generated wordlist from file, 9013 items...

Found bucket: hannstar.corporate-stage (404)

== S3scanner ==

S3Scanner [not found] : hannstar.com

擊中現有 S3 Bucket 清單：['hannstar.corporate-stage']

目的：防範錯誤配置，造成資料外洩

功能：從外部 NB 掃描 S3 Bucket 是否有被 Public 到外網

AWS雲端專案 – Team主動推送（雲端帳號掃描）

 ELK-ALERT 上午 10:10



雲端帳號盤點報告(AWS + GCP + GitLAB)

雲端帳號在 **AD** 狀態(判斷是否離職)

告警等級：正常     

使用者名稱: [redacted], 註解: [redacted], 帳戶到期: 從不,

使用者名稱: [redacted], 註解: [redacted], 帳戶到期: 從不,

使用者名稱: [redacted], 註解: [redacted], 帳戶到期: 從不,

使用者名稱: [redacted], 註解: [Title] 使用者不在 **AD** 內，此為 **APP Store** 帳號, 帳戶到期: **NONE**,

使用者名稱: [redacted], 註解: [Title] 使用者不在 **AD** 內，此為 **BCP** 備份帳號, 帳戶到期: **NONE**,

使用者名稱: [redacted], 註解: [redacted], 帳戶到期: 從不,

目的：防範員工離職後，雲端帳號沒有即時刪除

功能：將雲端(AWS, GCP, GitLAB)帳號去重複化後，每日詢問 AD 帳號是否存在

AWS雲端專案 – 資源監控



藉由自製的監控程式與結合雲原生的安全機制

來達到快速監控使用者操作行為與分析資源是否被挖礦等狀況

AWS雲端專案 – Team主動推送(核心服務數量&組態)

AWS 監控資源告警

40 分鐘內 AWS 服務：EC2

告警等級：警告 ⚡ ⚡ ⚡ ⚡ ⚡

訊息內容：[RED] 資源數量確認：EC2 有变动

新增> "i-05ea5814eefb58d71"

新增> "i-08d5446ece4e49637"

刪除< "i-04a3dedd80c243a53"

刪除< "i-09ef40319ced31c07"

AWS 監控資源告警

40 分鐘內 AWS 服務：Lambda

告警等級：警告 ⚡ ⚡ ⚡ ⚡ ⚡

訊息內容：[RED] Lambda Function: "test" 於 Region: us-west-2 在过去的 40 分钟内有变动。

目的：核心資源異動時告知，精簡監控人力外，可以知道是否有被亂開資源

功能：針對核心資源(IAM, S3, Lambda, RDS, EC2, SG)，如果發現數量異動，或是組態變更，主動推送通知

AWS雲端專案 – Team主動推送 (SSM)

allen-test 上午 10:01

新增

AWS EC2 OS 高風險指令 (30分鐘內)

高風險指令：sudo

告警等級：警告 🔥🔥🔥🔥

訊息內容：[{'sudo', 'message': {'eventVersion': '1.0', 'eventTime': '2024-07-29T01:43:11Z', 'awsRegion': 'us-west-2', 'target': {'id': 'i-06b97219331536b7a'}, 'userIdentity': {'arn': 'arn:aws:iam::571586012653:user/centerchen'}, 'runAsUser': 'ssm-user', 'sessionId': 'centerchen-jn4fkrxovyuraguml3buwqc3hm', 'sessionData': ['\\[?2004l\\[?2004h\\]0:ssm-user@chatbot-qas: ~\\[01;32mssm-user@chatbot-qas\\[00m:\\[01;34m~\\[00m\$ \\[K\\]0:ssm-user@chatbot-qas: ~\\[01;32mssm-user@chatbot-qas\\[00m:\\[01;34m~\\[00m\$ sudo su - ld0010']}]

說明：AWS System Manager 可以透過 EC2 內的 SSM agent，開啟 WEB Terminal 的功能，藉此取代 SSH 的功能，也可同時防止 SSH&SCP 疑慮與增加 MFA 保護

目的：補強 CloudTrail 無法紀錄 OS 內操作的指令，是否有高風險指令

功能：自訂高風險行為，當擊中定義行為時，主通推送告警，並變更告警等級

工作階段 ID：allenchiu-3tyd4bnz2hjyr7nog4svoz3rfa

執行個體 ID：i-0281058ec53ffd5cc

```
exec /bin/bash

cd
sh-5.2$ exec /bin/bash
[ssm-user@it-deploy bin]$
[ssm-user@it-deploy bin]$ cd
[ssm-user@it-deploy ~]$ ll
total 0
-rw-rw-r--. 1 ssm-user ssm-user 0 Jun 26 09:32 allen
[ssm-user@it-deploy ~]$
```


AWS雲端專案 – Team主動推送 (SSM)

功能：事後查詢

CloudWatch > 日誌群組 > SSM > All events

日誌事件

您可以使用下面的篩選條件來搜尋和比對日誌事件中的術語、短語或值。 [進一步了解篩選條件模式](#)

🔍 "rm" X 清除 1分鐘 30分鐘 1小時 12小時 自訂 網 UTC 時區 顯示 ▾

▶	時間戳記	訊息	日誌串流名稱
▼	2024-06-26T02:01:20.397Z	<pre>{ "eventVersion": "1.0", "eventTime": "2024-06-26T02:01:20Z", "awsRegion": "us-west-2", "target": { "id": "i-0281058ec53ffd5cc" }, "userIdentity": { "arn": "arn:aws:iam::571586012653:user/mingshih" }, "runAsUser": "ssm-user", "sessionId": "mingshih-4h6nf3yr5wvzuoarmvdb3d2r4", "sessionData": ["\u001b[0;jenkins@it-deploy:~\u0007\u001b[?2004h[jenkins@it-deploy ~]\$ rm Wordpress-DEV/ var -r"] }</pre>	mingshih-4h6nf3yr5wvzuoarmvdb3d2r4
▶	2024-06-26T07:47:13.004Z	<pre>{ "eventVersion": "1.0", "eventTime": "2024-06-26T07:47:13Z", "awsRegion": "us-west-2", "target": { "id": "i-0281058ec53ffd5cc" }, "userIdentity": { "arn": "arn:aws:iam::571586012653:user/mingshih" }, "runAsUser": "ssm-user", "sessionId": "mingshih-5lwnfzqhpz5dy5dm4pdfgqcjxq", "sessionData": ["\u001b[0;jenkins@it-deploy:~\u0007\u001b[?2004h[jenkins@it-deploy ~]\$ rm Wordpress-DEV/ var -r"] }</pre>	mingshih-5lwnfzqhpz5dy5dm4pdfgqcjxq
▶	2024-06-26T09:09:33.175Z	<pre>{ "eventVersion": "1.0", "eventTime": "2024-06-26T09:09:33Z", "awsRegion": "us-west-2", "target": { "id": "i-0281058ec53ffd5cc" }, "userIdentity": { "arn": "arn:aws:iam::571586012653:user/mingshih" }, "runAsUser": "ssm-user", "sessionId": "mingshih-zazeql4dukqr454yc4okqjwes4", "sessionData": ["\u001b[0;jenkins@it-deploy:~\u0007\u001b[?2004h[jenkins@it-deploy ~]\$ rm Wordpress-DEV/ var -r"] }</pre>	mingshih-zazeql4dukqr454yc4okqjwes4
▶	2024-06-27T05:36:45.381Z	<pre>{ "eventVersion": "1.0", "eventTime": "2024-06-27T05:36:45Z", "awsRegion": "us-west-2", "target": { "id": "i-0281058ec53ffd5cc" }, "userIdentity": { "arn": "arn:aws:iam::571586012653:user/mingshih" }, "runAsUser": "ssm-user", "sessionId": "mingshih-wrwnpkzdai4vomyk5k5c6i6y", "sessionData": ["\u001b[0;jenkins@it-deploy:~\u0007\u001b[?2004h[jenkins@it-deploy ~]\$ rm Wordpress-DEV/ var -r"] }</pre>	mingshih-wrwnpkzdai4vomyk5k5c6i6y
▶	2024-06-27T05:36:45.382Z	<pre>{ "eventVersion": "1.0", "eventTime": "2024-06-27T05:36:45Z", "awsRegion": "us-west-2", "target": { "id": "i-0281058ec53ffd5cc" }, "userIdentity": { "arn": "arn:aws:iam::571586012653:user/mingshih" }, "runAsUser": "ssm-user", "sessionId": "mingshih-wrwnpkzdai4vomyk5k5c6i6y", "sessionData": ["\u001b[0;jenkins@it-deploy:~\u0007\u001b[?2004h[jenkins@it-deploy ~]\$ rm Wordpress-DEV/ var -r"] }</pre>	mingshih-wrwnpkzdai4vomyk5k5c6i6y
▶	2024-06-28T02:52:34.713Z	<pre>{ "eventVersion": "1.0", "eventTime": "2024-06-28T02:52:34Z", "awsRegion": "us-west-2", "target": { "id": "i-0281058ec53ffd5cc" }, "userIdentity": { "arn": "arn:aws:iam::571586012653:user/mingshih" }, "runAsUser": "ssm-user", "sessionId": "mingshih-357bvvk2dmbxhrg6jhs3syh4sm", "sessionData": ["\u001b[0;jenkins@it-deploy:~\u0007\u001b[?2004h[jenkins@it-deploy ~]\$ rm Wordpress-DEV/ var -r"] }</pre>	mingshih-357bvvk2dmbxhrg6jhs3syh4sm

AWS雲端專案 – Team主動推送 (CloudTrail)

AWS Resources - CloudTrail 告警

AWS Console 異常動作告警(15分鐘內)

告警等級：危險 🔥 🔥 🔥 🔥 🔥

異常動作：

RegisterTargets

CreatePolicyVersion

DeletePolicyVersion

說明：CloudTrail 是可紀錄使用者、角色或 AWS 服務所執行的動作會記錄為中的事件。

事件包括在 AWS Management Console、AWS Command Line Interface和 AWS SDK 和 API 中採取的動作。

目的：監控操作人員行為安全性，補強上一頁自製監控無法觀測行為(ex.隨意關閉 EC2 主機)

功能：自訂高風險行為，當擊中定義行為時，主通推送告警，並變更告警等級

AWS雲端專案 – 定時報表



定時推送的彙整報表，得知服務呼叫量與
在線使用者

藉此可達到服務是否合理的使用，與活躍
的使用者是否正確

AWS雲端專案 – Team主動推送 (Report)

定時掃描結果概覽

AWS Resource 使用資訊(最近 1 小時)

告警等級：正常 ✓✓✓✓✓

被呼叫的服務名(22)

config.amazonaws.com
xray.amazonaws.com
ssm.amazonaws.com
sts.amazonaws.com
cloudtrail.amazonaws.com
s3.amazonaws.com
kms.amazonaws.com
tagging.amazonaws.com
backup.amazonaws.com
ec2.amazonaws.com
logs.amazonaws.com
iam.amazonaws.com
lambda.amazonaws.com
rds.amazonaws.com
wafv2.amazonaws.com
cloudformation.amazonaws.com
events.amazonaws.com
resource-groups.amazonaws.com
dynamodb.amazonaws.com
ecs.amazonaws.com
elasticmapreduce.amazonaws.com
personalize.amazonaws.com

活動中使用者(2)

bcp-backup
allenchiu

aws_config
監控資源(最近 20 分鐘)

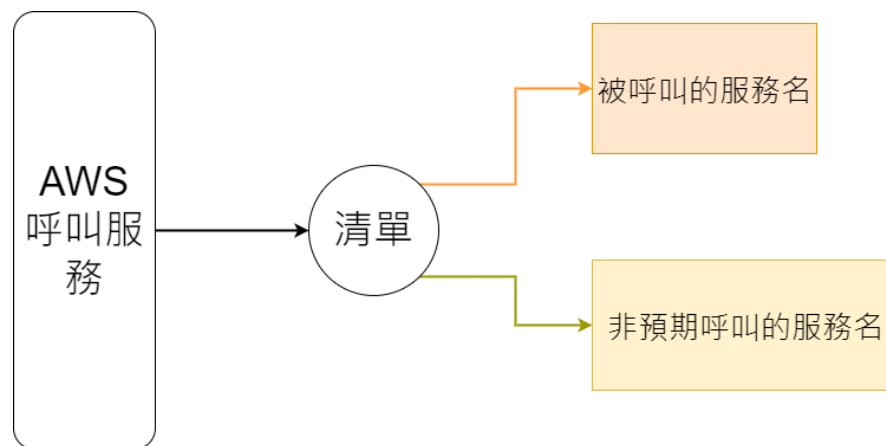
AWS EC2 數量： 34 (Running: 12 , Stopped: 22)
AWS IAM 數量： 11
AWS RDS 數量： 2
AWS SG 數量： 44
AWS Lambda 數量： 12

非預期呼叫服務(0)

目的：每小時回報監控狀態，並可藉此查看，是否有不該出現的使用者(ex.被盜用或突然未曾出現的帳號)，與未曾使用的服務(ex.被挖礦開啟的服務)

功能：報表將呈現

- 1.核心資源數量
- 2.被呼叫的服務名稱(已於安全列表中註記的)
- 3.目前正在操作的使用者
- 4.不在安全列表中的服務



AWS雲端專案 – 跟 SIEM 的差異



SIEM是一種解決方案，能協助組織在威脅傷害企業營運前，搶先偵測、分析和回應安全性威脅。

一般都會提供這些核心功能：

- 記錄管理：SIEM 系統會將大量資料集中在一個地方，並整理和判斷資料是否有威脅、攻擊或入侵的跡象。
- 事件關聯性：系統會排序資料以識別其關係和模式，來快速偵測和回應潛在的威脅。
- 事件監控和回應：SIEM 技術會跨組織網路監控安全性事件，並提供與事件相關的所有活動警示與稽核。

SIEM 系統可以透過各種使用案例來緩解網路風險，像是偵測可疑的使用者活動、監控使用者行為、限制嘗試存取並產生合規性報告。

目前我的專案，僅有包含 Log 紀錄收集，然後針對收集 Log 做關鍵字查詢做告警，缺少情資分析與合規性，事件關聯性等核心功能