網路與系統安全-期末作業

1. 作業 1

作業 1-1 MIMECAST 安全漏洞之探討

作業連結
:https://drive.google.com/file/d/1dhTXIBed2uvdHzSa4V_Zpmg9J_E_LqqX/view?usp=sharing

作業 1-2 MIMECAST-資安健檢

作業連結:
https://drive.google.com/file/d/1yH7T0WWhh-roKKrJ_HOZ7RvS6PQ1HYaY/view?usp=sharing

2. 作業 2

作業 2-1 運用 elasticsearch 資料分析輸出一個 2 維圖

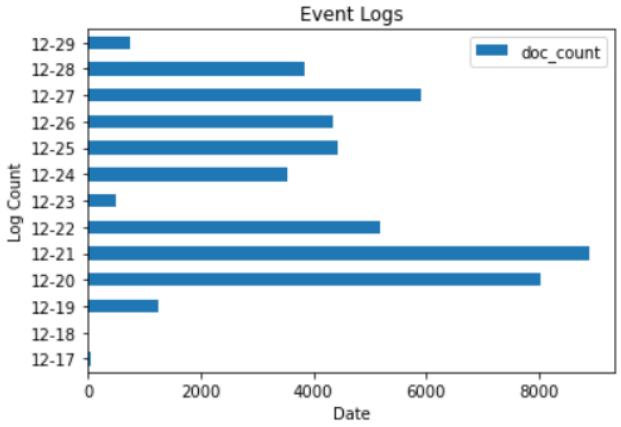
說明:連結 Elasticsearch 讀取 winlogbeat 資料 K831130BMs_nTerjfMVt。

```
In [1]: from datetime import datetime
        from elasticsearch import Elasticsearch
        import matplotlib.pyplot as plt
        import pandas as pd
        import requests
        import time

In [2]: es_ip = "http://127.0.0.1:9200"

In [3]: es = Elasticsearch(es_ip)

In [4]: res = es.get(index="winlogbeat", id="K831130BMs_nTerjfMVt")
        print(res['_source'])
```

{'@timestamp': '2021-12-20T12:51:18.229Z', 'ecs': {'version': '1.9.0'}, 'agent': {'type': 'winlogbeat', 'version': '7.13.2', 'hostname': 'DESKTOP-T3V8EOP', 'ephemeral_id': '41f4d791-f3b8-47ed-b193-c7151f023406', 'id': '621af60c-6ab1-4b77-803e-d523c7d8ec04', 'name': 'DESKTOP-T3V8EOP'}, 'event': {'created': '2021-12-20T12:51:20.151Z', 'code': '1', 'kind': 'event', 'provider': 'Microsoft-Windows-Sysmon', 'timezone': '+08:00'}, 'log': {'level': 'information'}, 'host': {'architecture': 'x86_64', 'os': {'name': 'Windows 10 Pro', 'kernel': '10.0.22000.318 (WinBuild.160101.0800)', 'build': '22000.318', 'type': 'windows', 'platform': 'windows', 'version': '10.0', 'family': 'windows'}, 'id': '1f725ed7-b14c-494d-9fc1-4bc3eeb0b29b', 'ip': ['fe80::1911:e65c:d649:9768', '192.168.56.1', 'fe80::24c3:baf3:3d58:f2af', '169.254.242.175', 'fe80::a832:f35:3de:862c', '169.254.134.44', 'fe80::d4a8:14f8:2744:a74a', '192.168.0.83', 'fe80::4d6b:1d3e:cee1:343d', '169.254.52.61'], 'name': 'DESKTOP-T3V8EOP', 'mac': ['0a:00:27:00:00:10', '24:ee:9a:ff:17:da', '26:ee:9a:ff:17:d9', '24:ee:9a:ff:17:d9', '24:ee:9a:ff:17:dd'], 'hostname': 'DESKTOP-T3V8EOP'}, 'winlog': {'event_id': '1', 'user': {'identifier': 'S-1-5-18', 'domain': 'NT AUTHORITY', 'name': 'SYSTEM', 'type': 'User'}, 'event_data': {'ProcessGuid': '{1f725ed7-7c46-61c0-361b-938100000000}', 'Company': 'Rivet Networks LLC', 'LogonId': '0x6ba12a0f', 'TerminalSessionId': '2', 'IntegrityLevel': 'Medium', 'Hashes': 'MD5=F70A23758DA94B90A01CC791ACC7F385,SHA256=EEBCC0C6FD9A7BF70BA3028DAEA19C450FCC698169C2E5B03F6BEF9D4BBA1A6F,IMPHASH=935B686812E8D4246E2278AF50AA30FB', 'ParentProcessId': '5312', 'ParentCommandLine': '"RAPS.exe"', 'UtcTime': '2021-12-20 12:51:18.228', 'FileVersion': '3.1.995.0', 'ProcessId': '13720', 'OriginalFileName': 'RAPS.exe', 'User': 'DESKTOP-T3V8EOP\\a3789', 'CommandLine': 'RAPS.exe -u', 'CurrentDirectory': 'C:\\Program Files\\Rivet Networks\\SmartByte\\', 'ParentImage': 'C:\\Program Files\\Rivet Networks\\SmartByte\\RAPS.exe', 'Description': 'RivetAPS', 'LogonGuid': '{1f725ed7-4242-61bc-0f2a-a16b00000000}', 'ParentProcessGuid': '{1f725ed7-296e-61ab-8f00-000000000d00}', 'RuleName': '-', 'Image': 'C:\\Program Files\\Rivet Networks\\SmartByte\\RAPS.exe', 'Product': 'RivetAPS'}, 'version': 5, 'api': 'wineventlog', 'channel': 'Microsoft-Windows-Sysmon/Operational', 'provider_name': 'Microsoft-Windows-Sysmon', 'record_id': 496, 'computer_name': 'DESKTOP-T3V8EOP', 'provider_guid': '{5770385f-c22a-43e0-bf4c-06f5698ffbd9}', 'process': {'thread': {'id': 26096}, 'pi

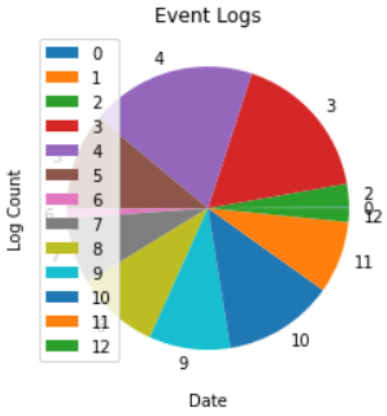
說明:輸出二維圖-橫條圖

```
In [19]: event_pd = pd.DataFrame(result, columns=["key_as_string", "doc_count"])
         #print(event_pd)
         event_pd.plot(x="key_as_string", y="doc_count", kind="barh");
         plt.xlabel('Date')
         plt.ylabel('Log Count')
         plt.title('Event Logs')

Out[19]: Text(0.5, 1.0, 'Event Logs')
```



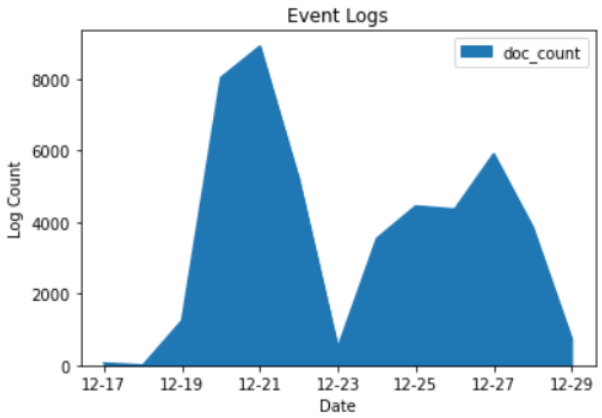
說明:輸出二維圖-圓餅圖

```
In [12]: event_pd = pd.DataFrame(result, columns=["key_as_string", "doc_count"])
         #print(event_pd)
         event_pd.plot(x="key_as_string", y="doc_count", kind="pie");
         plt.xlabel('Date')
         plt.ylabel('Log Count')
         plt.title('Event Logs')

Out[12]: Text(0.5, 1.0, 'Event Logs')
```



說明:輸出二維圖-區域圖

```
In [16]: event_pd = pd.DataFrame(result, columns=["key_as_string", "doc_count"])
         #print(event_pd)
         event_pd.plot(x="key_as_string", y="doc_count", kind="area");
         plt.xlabel('Date')
         plt.ylabel('Log Count')
         plt.title('Event Logs')

Out[16]: Text(0.5, 1.0, 'Event Logs')
```



作業 2-2 Log4j 漏洞探討

事件說明

Log4j 是一項透過 JAVA 開發，常用於偵錯，並可記錄資料並存於記錄檔中，也因此而形成日誌框架便利許多工程師，該服務被許多科技巨頭使用，並且全球有許多的企業使用。但近期發現該漏洞存在漏洞，能透過一行指令就能進入公司電腦任意攻擊或是獲取機密內容，該危害影響數百萬使用者。

解決辦法

自行防範措施

Step 1 :透過 Snky 等工具找出含有紕漏的程式碼與應用程式。

Step 2 :確認 log4j 的程式碼是否實際部屬到營運環境。

Step 3 :部屬還成後，這些紀錄功能就會關閉，避免漏洞造成影響。

官方措施-Apache 推出修復程式

Step 1 :下載最新版 Log4j

Step 2 :檢查 Apache Foundation 網站上的最新修正資訊

Step 3 :安裝 IPS 規則攔截 Log4j 的輸入字串

停用記錄檔功能，直到所有呼叫到 Log4j 的地方都標成註解

探討內容

許多的整合性服務，會指向某些功能提供者，並由他們提供的服務為基底，可以重這次事件發先，影響原因是因為許多公司行號系統皆使用這服務當作系統基底之一。

使用記錄服務本身沒有問題，這項動作本身就是為了便捷工程師使用，因此針對影響可以發現大公司在使用上並不能多數使用他人的服務。此次風險最大的為科技巨頭，因為他們擁有全世界用戶的多少個人資訊，並且其底下的公司也是數家，想當然功能性基底也會沿用，而使用他人提供的服務最為基底，的確可以省下許多成本，但公司規模的成長，勢必要採取替代避免為往後埋下風險的未爆彈。

舉例來說不論是 google、Apple，他們在許多硬體、軟體都已經開始採取自行研發。這動作有商業因素在，但也是資安的一種確保，減少波及性。這次 Apple 的雲端系統也有受影響，但是這也證實它們自行研發的動作是對的，若沒有將產品服務採取一條龍的內容，或許會引爆更多問題。因此公司在成立時可以透過使用他人提供的服務進行運作，但成長到一定規模後，可開始考慮一些服務的影響性及成本考量的權衡採取轉型搓施，避免資安問題帶來風暴性的風險，