程式驅動
code-driven

Splunk 教育訓練 2

7/26 案例主題：作業系統安全事件日誌

更了解Splunk

Splunk 重要專有名詞說明

程式驅動 code-driven

- Data Input : 資料輸入（例如：檔案、TCP、UDP、WMI、Script、Forwarder、Stream、API...）
- Source type ： 來源類別（例如：apache logs, security log、network log, sensor log...）
- Host ： 資料主機（例如：apache1、apche2, apserver1, firewall1, 10.1.1.2, ...)
- Source : 來源（例如：/opt/apache/log/*.*, udp:514, /bin/current_status.sh）
- Field : 欄位（字段）： 以正規表示式(Regular Expression) 擷取出欄位（字段）
- Search Language：搜尋語法（概念： 縮小範圍 -> 運算 -> 結果呈現 ）
- Saved Search： 儲存搜尋，將搜尋條件 存下來，下次可以直接用
- Alert : 告警，當 搜尋到特定關鍵字、統計分析達到設定值，可發出警告（即時、排程）
- Report ： 報表，將 儲存搜尋結果，產出的 圖形化報表
- Dashboard ： 儀表版，將不同報表彙整多個面板 成 儀表版
- Data Model : 資料模型，將機器資料虛擬化的資料結構
- Pivot Analysis : 樞紐分析，提供給 一般使用者 可以拖拉產生報表和儀表板

基本搜尋

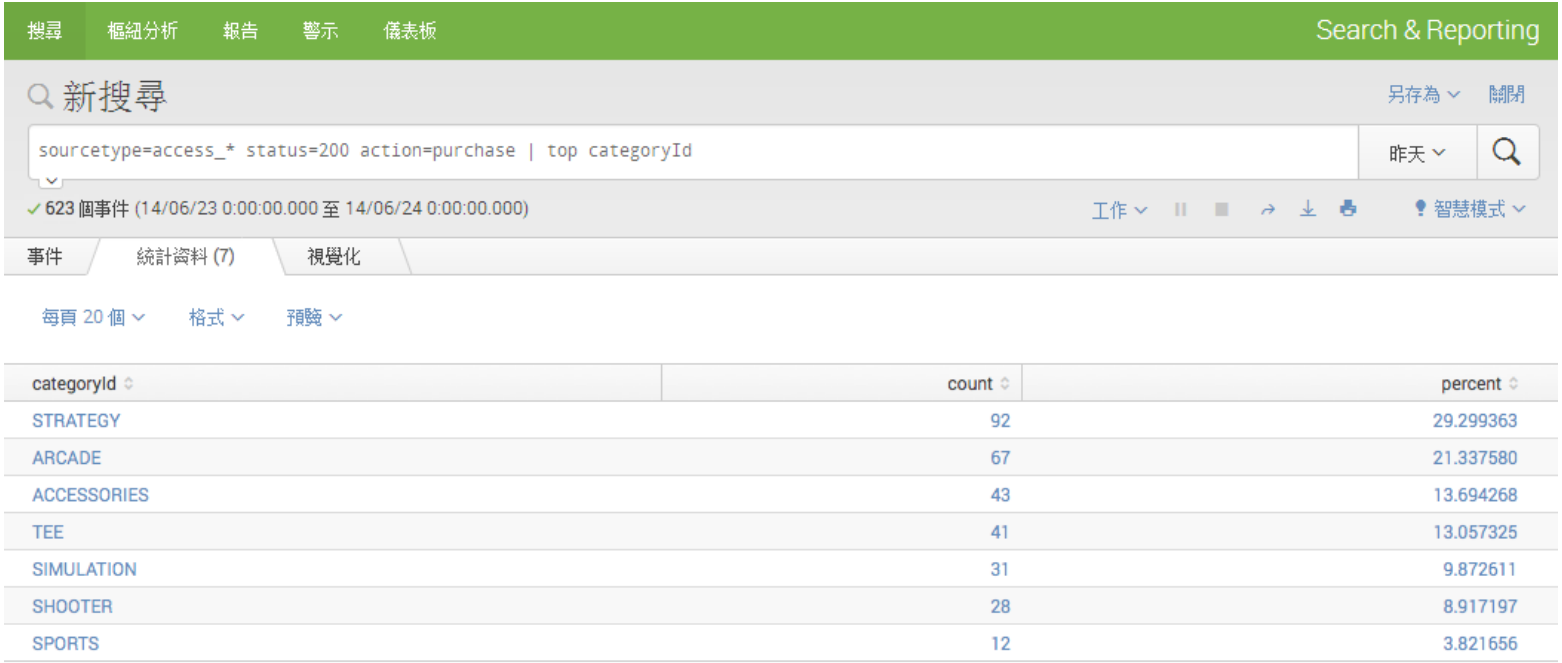
- **關鍵字Keywords**
  搜尋error, password
- **布林函數Booleans**
  OR, AND, NOT ; AND是默認值不顯示；必須為大寫，可將需優先執行條件放入( )中
  sourcetype=vendor_sales OR (sourcetype=access_combined action=purchase)
- **詞組Phrases**
  “web error”不同於web AND error
- **欄位搜尋Field serarches**
  status=404, user=admin
- **萬用字元Wildcards ***
  status=40* matches 40, 40a, 404 等等。關鍵字前面使用 * 是無效的如*dmin
- **比較Comparisons**
  =, !=, <, <=, >=, > status>399, user!=admin

語法概念

搜尋以五個元件組成

- Search terms — 你想看什麼？
  -關鍵字，詞句 ，布林函數等等
- Command — 你想對搜尋結果做些什麼？
  -建立圖表，計算統計，評估與格式化等等
- Function – 你想要對搜尋結果做如何圖表，計算與評估
  -加總，取平均值，轉換值等等
- Arguments — 有什麼變數要應用到這個功能？
  -計算特定欄位的平均值，轉換milliseconds to seconds等等
- Clauses — 你想要如何組合或重新命名搜尋結果中的欄位

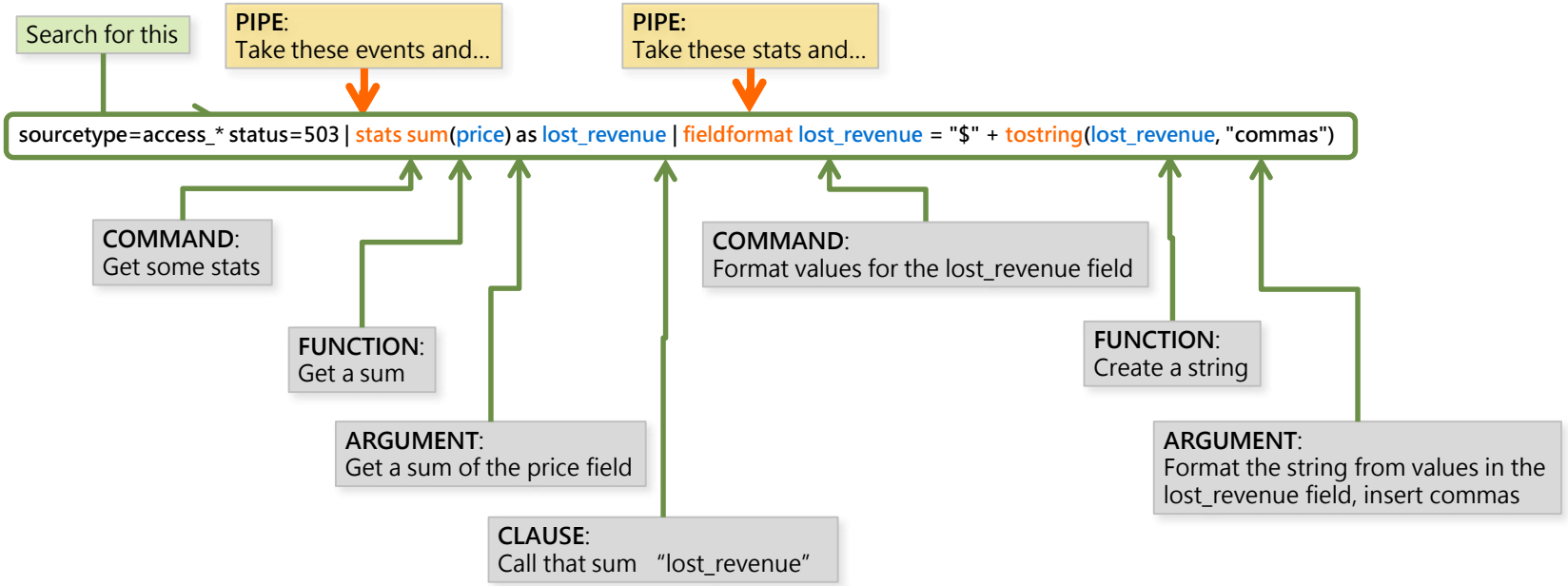
使用 直立線字元 | 來進行 資料的後續處理



categoryId	count	percent
STRATEGY	92	29.299363
ARCADE	67	21.337580
ACCESSORIES	43	13.694268
TEE	41	13.057325
SIMULATION	31	9.872611
SHOOTER	28	8.917197
SPORTS	12	3.821656

搜尋 語言 的 範例

This diagram represents a search, broken into its syntax components

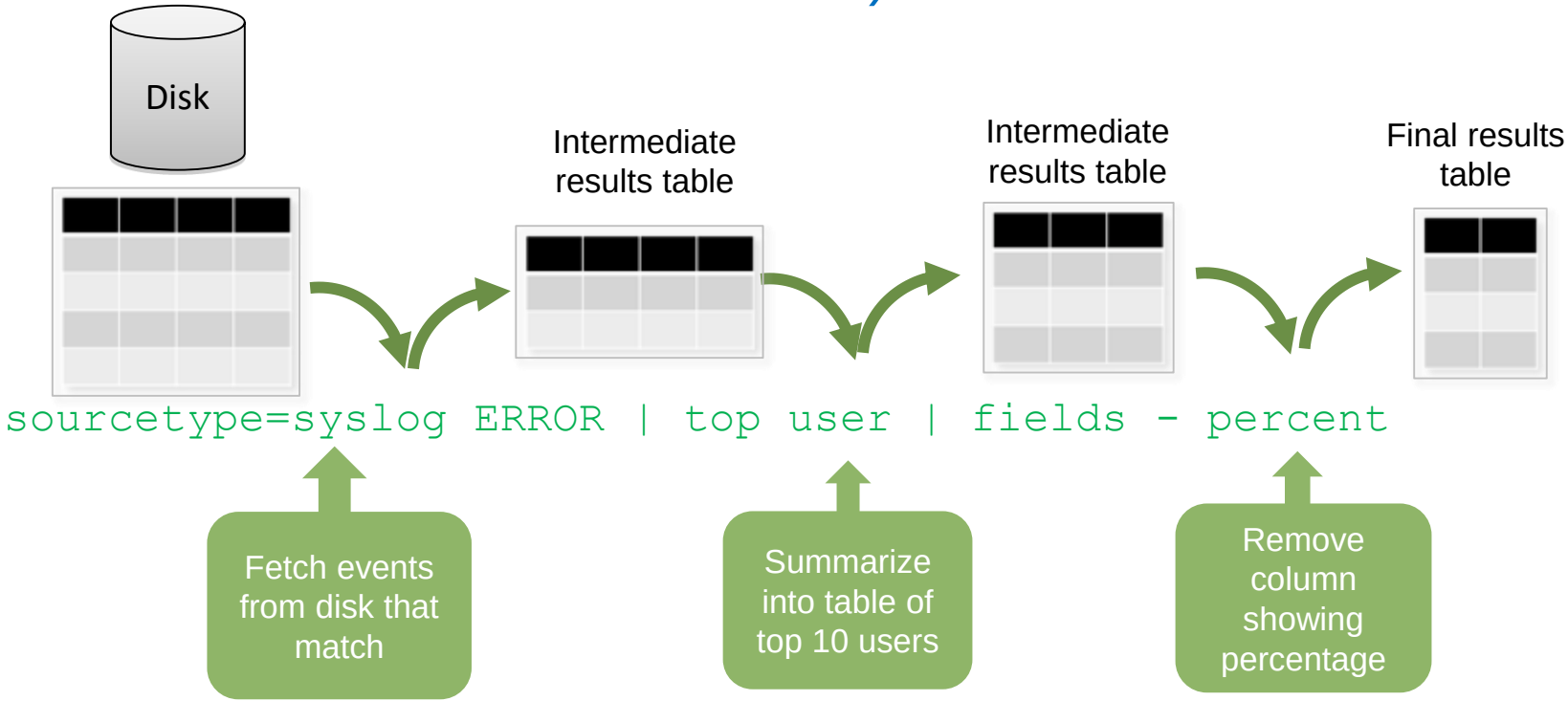


搜尋範例

程式驅動 code-driven

- 搜尋 Buttercup Games 商店的成功購買數
  - sourcetype=access_* status=200 action=purchase
- 搜尋 發生錯誤 的產生記錄
  - (error OR fail* OR severe) OR (status=404 OR status=500 OR status=503)
- 搜尋昨天購買了多少模擬遊戲
  - sourcetype=access_* status=200 action=purchase categoryId=simulation

搜尋語法處理的過程
(範圍縮小 => 運算 => 呈現)



Searching and Reporting

目標

程式驅動 code-driven

透過下列練習，熟悉source type
使用下列指令，產生搜尋內容

- -table
- -rename
- -field
- -dedup
- -sort

Searching & Reporting with Splunk

建立表單 Table

想知道網路的 src , dest, app 與 rule的相互關係，如何視覺化

Table命令用來回傳使用參數列表(src ,dest,app,rule)的欄位欄位表格 。

```
1 sourcetype="pan:threat"
2 | table src,src_port,dest,dest_port,app,rule
```

src	src_port	dest	dest_port	app
192.168.0.2	50297	184.106.31.170	80	web-browsing
72.21.194.1	80	192.168.0.2	59160	web-browsing
64.39.66.153	80	192.168.0.3	59310	web-browsing
192.168.0.2	62525	204.232.231.46	80	web-browsing
192.168.0.2	64276	184.106.31.170	80	web-browsing
192.168.0.3	8839	74.125.224.195	80	web-browsing
200.147.33.17	80	192.168.0.2	57451	web-browsing
222.222.204.67	80	192.168.0.2	50928	web-browsing
192.168.0.2	59709	213.180.199.61	80	web-browsing
192.168.0.2	58928	184.106.31.170	80	web-browsing
192.168.0.2	61425	64.74.223.43	80	web-browsing
192.168.0.2	57566	184.106.31.170	80	web-browsing

修改表單欄位名稱 Rename

客戶想知道網路 的 src , dest, app 與 rule的相互關係，如何視覺化

Rename命令用來將table回傳使用欄位更具意義。

```
rename src as 來源位置,
       dest as 目的位置
       app as 應用程式,
       rule as 規則
```

```
1 sourcetype="pan:threat"
2 | table src,src_port,dest,dest_port,app,rule
3 | rename src as 來源位置,
4         dest as 目的位置
5         app as 應用程式,
6         rule as 規則
```

來源位置	目的位置	應用程式	規則
192.168.0.2	184.106.31.170	web-browsing	rule1
192.168.0.2	64.78.56.109	ssl	rule1
192.168.0.2	204.232.231.46	web-browsing	rule1
192.168.0.2	204.232.231.46	web-browsing	rule1
192.168.0.2	212.193.230.207	web-browsing	rule1
200.147.1.41	192.168.0.2	web-browsing	rule1
192.168.0.2	218.94.11.45	web-browsing	rule1
192.168.0.2	184.106.31.170	web-browsing	rule1

極速搜尋 使用 Fields

欄位萃取是搜尋中最花資源的部分。
使用Field命令可以“包含”或“排除”特定的欄位，加速搜尋的效果。
使用“包含”會優於“排除”

splunk>

Searching & Reporting with Splunk

極速搜尋 使用 Fields

程式驅動 code-driven

客戶想知道網路 的 src , dest, app 與 rule的相互關係，如何視覺化

```
sourcetype="pan:threat"
| fields src,dest,app,rule
| table src,dest,app,rule
| rename src as 來源位置,
        dest as 目的位置
        app as 應用程式,
        rule as 規則
```

A rename productId as ProductID

B rename action as "Customer Action"

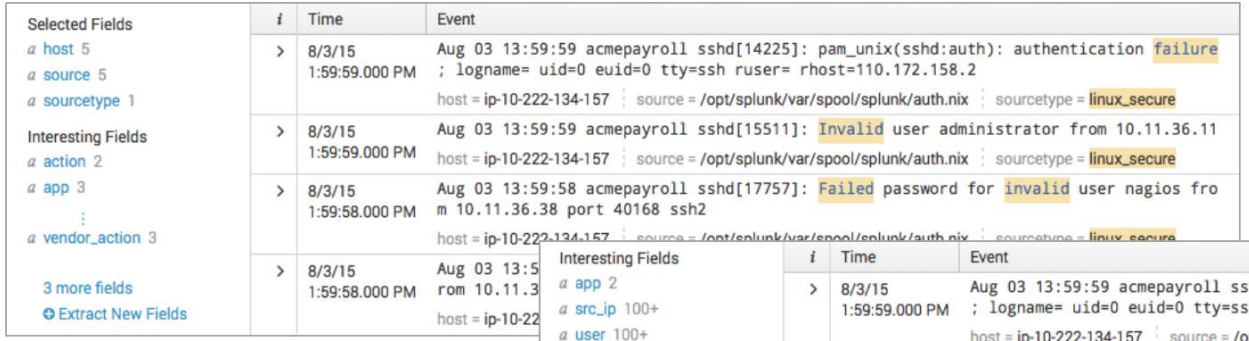
C rename status as "HTTP Status"

來源位置	目的位置	應用程式	規則
192.168.0.2	184.106.31.170	web-browsing	rule1
192.168.0.2	64.78.56.109	ssl	rule1
192.168.0.2	204.232.231.46	web-browsing	rule1
192.168.0.2	204.232.231.46	web-browsing	rule1
192.168.0.2	212.193.230.207	web-browsing	rule1
200.147.1.41	192.168.0.2	web-browsing	rule1
192.168.0.2	218.94.11.45	web-browsing	rule1
192.168.0.2	184.106.31.170	web-browsing	rule1

極速搜尋 使用 Fields

客戶想知道上週發生網路問題的狀況，針對user, app,與src_ip上的欄位進行萃取

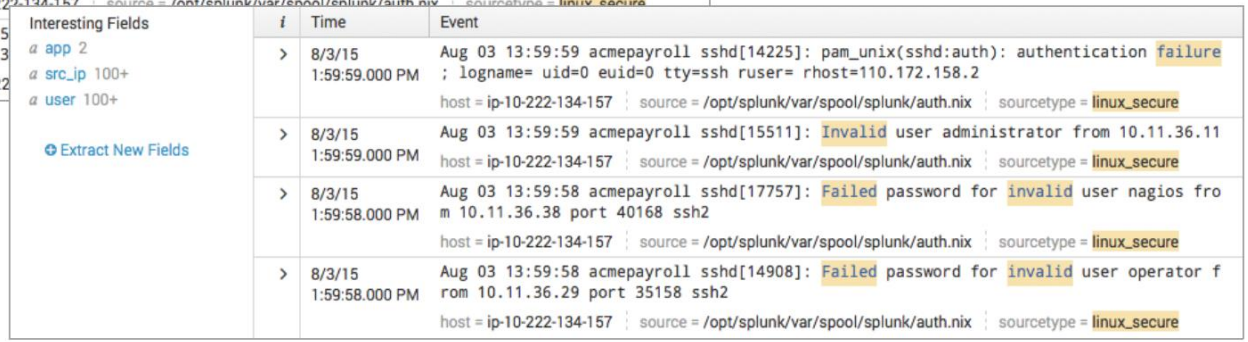
提升效率----只有萃取特定需要的欄位



Returned **6,567** results by scanning **6,567** events in **1.425** seconds.

```
sourcetype=linux_secure
  (fail* OR invalid)
| fields user, app, src_ip
```

A



Returned **6,567** results by scanning **6,567** events in **0.753** seconds.

重複資料刪除Dedup

從搜尋的結果移除重複資料

```
1 sourcetype="pan:threat"
2 | table category,app,rule,action
```

category	app	rule	action
health-and-medicine	web-browsing	rule1	allowed
business-and-economy	web-browsing	rule1	allowed
social-networking	web-browsing	rule1	allowed
malware-sites	web-browsing	rule1	blocked
any	web-browsing	rule1	blocked
any	web-browsing	rule1	blocked
not-resolved	web-browsing	rule1	allowed

| dedup category

category	app
malware-sites	web-browsing
business-and-economy	web-browsing
not-resolved	web-browsing
any	web-browsing

| dedup category , app

category	app
web-hosting	web-browsing
web-advertisements	web-browsing
not-resolved	web-browsing
malware-sites	web-browsing

使用Sort排序結果

使用升序 + ascending由小到大(預設)
或 降序 - descending由大到小
限制回傳結果的數量，使用limit參數

```
... | sort limit=20 -categoryId, product_name
... | sort 20 count
```

使用Sort排序結果

由小到大(預設) 或 由大到小

```
1  sourcetype="pan:threat"
2  | table category,app,rule,action
3  | dedup category,app
4  | sort limit=20 -category,+app,rule,action
```

category	app	rule	action
web-hosting	ssl	rule1	allowed
web-hosting	web-browsing	rule1	allowed
web-based-email	hotmail	rule1	allowed
web-based-email	mail.ru-base	rule1	allowed
web-based-email	ssl	rule1	allowed
web-based-email	web-browsing	rule1	allowed

轉換指令 得出統計資料

程式驅動 code-driven

將搜索結果轉換到Splunk可用於統計的數據表中
需要將搜索結果轉換為可視化

學會使用以下命令及其功能

- top
- rare
- stats

splunk>

Searching & Reporting with Splunk

使用top指令

在一個小時前，應用程式使用最多

top指令將搜索結果找到欄位最常見的值並計數，轉換至欄位
–預設回傳最常見的10筆結果

app	count	percent
web-browsing	119995	93.210135
google-maps	2618	2.033619
ssl	2192	1.702709
facebook-base	1244	0.966319
google-analytics	825	0.640846
flash	419	0.325472
sourceforge	329	0.255562
pandora	275	0.213615
google-safebrowsing	142	0.110303
apple-update	131	0.101759

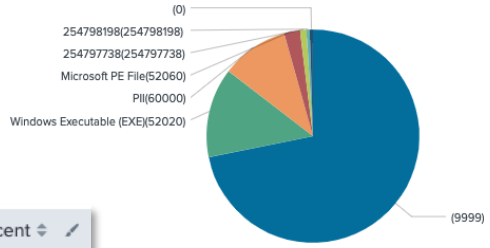
使用top指令

- 預設輸出顯示為表格格式
- 自動回傳**count** 與**percent**列。
- Limit=# 回傳這個數量的結果
  - –預設顯示10筆最常見的結果
  - –limit=0則為顯示全部結果數量
- **countfield=字串**提供將原本count欄位的名稱改變成所需的名字。
- **showperc=f** 將不建立percent欄位。

使用Top指令

在一個小時前，產生最多的攻擊事件的前20名威脅是什麼

```
1  sourcetype="pan:threat"
2  | top limit=20 threat
```



threat	count	percent
(9999)	89055	70.975429
Windows Executable (EXE)(52020)	20200	16.099081
PII(60000)	12033	9.590111
Microsoft PE File(52060)	2005	1.597953
(0)	245	0.195261
Adobe Portable Document Format (PDF)(52021)	148	0.117954
256429558(256429558)	129	0.102811
254799658(254799658)	128	0.102014
254796918(254796918)	120	0.095638

使用rare指令

在過去一個小時內，哪一個行為最少出現在你的網路環境中？

rare指令將搜索結果找到欄位最少見的值並計數，轉換至欄位

–預設回傳最常見的10筆結果

–相關參數與 top用法一致

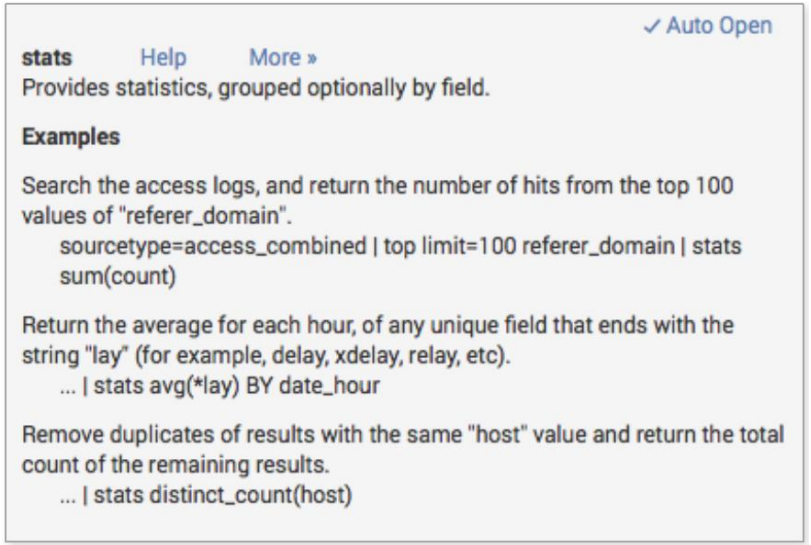
```
1  sourcetype="pan:threat"
2  | rare showperc=f limit=20 threat
```

threat	count
Antivirus 2009 Downloads Antivirus Executable(12466)	1
HTML/Trojan.agent.cqbon(255147)	1
Antivirus-2010 asking download from tbest-antivirus-2010-download.info(12507)	3
Trojan.Win32.Ertfor.A updatesabout.com(12587)	3
Bredolab.Gen Command and Control Traffic(13024)	4
Trojan-Downloader.Win32.Zlob.wwv runtime childhe(12471)	4
Win PC Defender runtime detection(12548)	4
Trojan-Spy.Win32.Zbot.wti(12620)	6
Antivirus-2009 redirect to order page(12402)	14

使用stats指令

- stats讓你可以針對搜尋條件產生的結果進行統計計算。
- 常見function 包含以下：

-count – 回傳搜尋條件匹配的事件數量
-sum – 回傳數字加總
-avg –回傳數字平均
-list – 回傳欄位內所有的值
-values – 回傳欄位內的唯一值



使用stats指令count功能

想看到60分鐘有Malware活動的來源IP統計

```
1 sourcetype="pan:threat" "tag::eventtype"=malware
2 | stats count by src
```

src	count
112.175.39.123	9
187.73.33.50	7
188.138.1.135	13

- 使用as可以將count 欄位名稱改成更易懂的名稱

```
1 sourcetype="pan:threat" "tag::eventtype"=malware
2 | stats count as 次數 by src
3 | rename src as 來源位置
```

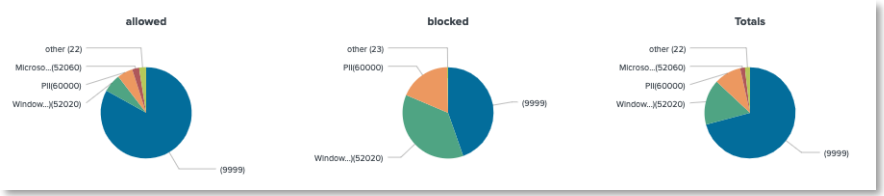
來源位置	次數
112.175.39.123	9
187.73.33.50	7
188.138.1.135	13
205.185.216.10	10
213.186.33.4	10

使用stats指令count（欄位）

想看到15分鐘前威脅事件，防火牆的威脅對映動作Allow,Block及全部事件統計

- 加一個欄位名稱當做參數，計算相關的事件數量與百分比。
- 使用as可以將count 欄位名稱改成更易懂的名稱。

```
1  sourcetype="pan:threat"
2  | stats count(eval(action="allowed")) as allowed ,
3          count(eval(action="blocked")) as blocked ,
4          count as Totals by threat
5  | sort - Totals
```



threat	allowed	blocked	Totals
(9999)	6932	1737	8669
Windows Executable (EXE)(52020)	538	1429	1967
PII(60000)	457	713	1170
Microsoft PE File(52060)	205	0	205
(0)	37	0	37
254797738(254797738)	17	0	17

使用stats指令count by 欄位

程式驅動 code-driven

想看到15分鐘前根據來源與目的分類產生威脅的事件數量

- 經由子句回傳一個指定欄位或欄位組的事件數量統計
- 可使用任意數量的欄位當參數透過by欄位列舉

–與chart/timechart指令基本不同為，chart/timechart可使用的欄位限制為2

```
1 sourcetype="pan:threat"
2 | stats count as Count by threat,src,dest
3 | sort - Count
```

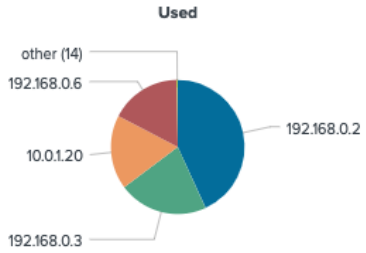
threat	src	dest	Count
(9999)	192.168.0.2	184.106.31.170	3436
(9999)	192.168.0.2	204.232.231.46	1004
(9999)	192.168.0.2	208.73.210.29	171
PII(60000)	72.21.194.1	192.168.0.2	115
(9999)	192.168.0.2	64.78.56.109	111
PII(60000)	74.125.224.200	192.168.0.2	111
(9999)	192.168.0.2	17.254.32.16	107
Windows Executable (EXE)(52020)	200.147.33.17	192.168.0.2	106
Windows Executable (EXE)(52020)	200.147.33.19	192.168.0.2	103

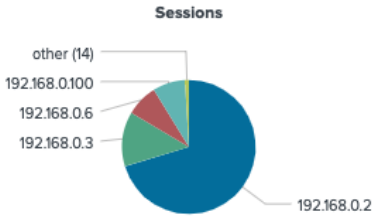
使用stats指令 sum（欄位）

想知道上週使用公司網路使用流量跟連線數

欄位內容為數字可用sum做加總的動作

```
1 sourcetype="pan:traffic"
2 | stats sum(bytes) as Used , count by src
3 | sort - Used
```





src	Used	count
192.168.0.2	99748383	6175
192.168.0.3	49521977	1149
10.0.1.20	44225409	34
192.168.0.6	41225619	686
192.168.0.100	349508	687
108.224.90.120	94346	1

使用stats指令 avg（欄位）進階

想知道上週使用公司網路使用流量跟平均使用量

```
1 sourcetype="pan:traffic"
2 | stats sum(bytes) as Used ,
3         avg(bytes) as "Avg Used",
4         count as Sessions by src
5 | sort - Used
```

欄位內容為數字可用avg
做計算平均值的動作

src	Used	Avg Used	Sessions
192.168.0.2	70580346	11422.61628095161	6179
192.168.0.3	46088543	40393.11393514461	1141
10.0.1.20	45724410	1270122.5	36
192.168.0.6	40119289	60879.04248861912	659
192.168.0.100	336545	494.91911764705884	680
108.224.90.120	94346	94346	1
98.248.152.109	26904	13452	2
192.168.0.1	21370	1017.6190476190476	21
166.205.139.177	5635	1127	5

使用stats指令 values（欄位）

想知道4小時威脅分數為4,5使用的IP跟User的關係

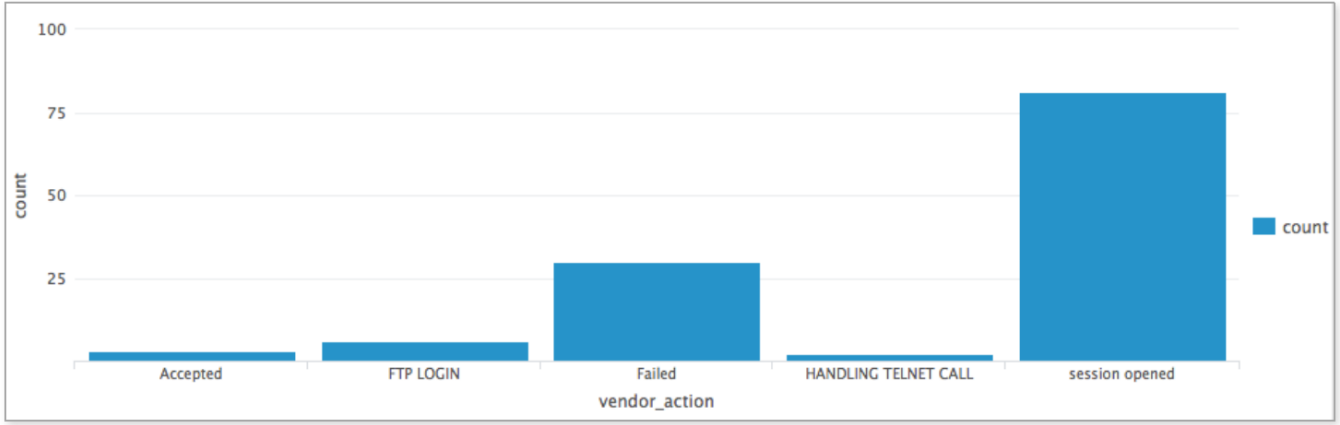
```
1  sourcetype="pan:threat" app:risk=4 OR app:risk=5
2  | stats values(user) as Users ,count by src
```

src	Users	count
10.0.1.20	tng\crusher tng\jordy tng\picard	116
109.201.131.15	crusher tng\crusher	134
109.235.249.163	crusher tng\crusher	53
112.175.39.123	tng\crusher	327
114.108.168.12	crusher tng\crusher	103

資料結構化

- 大多數將搜尋結果可視化，至少會結構化成兩列的表格。
- 在圖表中
  - 第一列提供X軸的值
  - 第二列提供Y軸的值

vendor_action	count
Accepted	2
FTP LOGIN	6
Failed	29
HANDLING TELNET CALL	2
Invalid user	3
session opened	59



資料結構化chart

- Chart指令可以顯示任何一系列的圖表
- 你可以決定x軸是使用哪個欄位繪製於圖表中
  - –相關的參數顯示視為Y軸，必須要為數字
  - –使用的第一個欄位在over參數後的視為X軸
  - –使用over與by將數據分成子分組，相關的內容將產生於該圖表中

chart avg(bytes) over host

- –host 值會於X軸

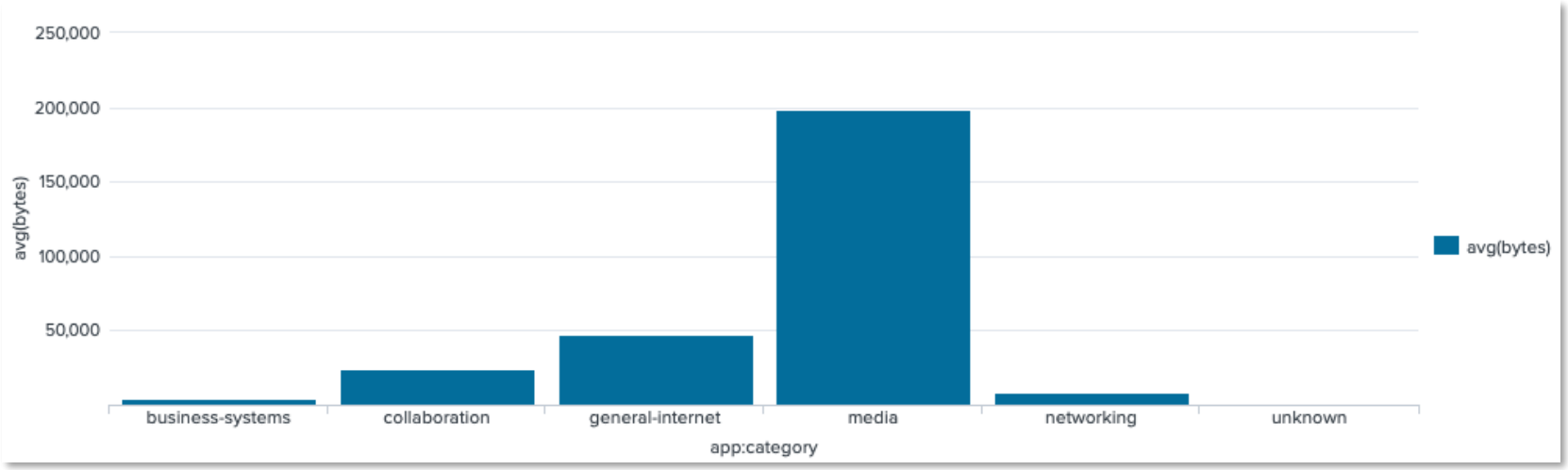
chart avg(bytes) over host by product_name

- –host 值會於X軸，在product_name進行x軸拆分

資料結構化chart over欄位

顯示24小時內應用程式類別分析圖

```
1  sourcetype="pan:traffic"
2  | chart avg(bytes) over app:category
```

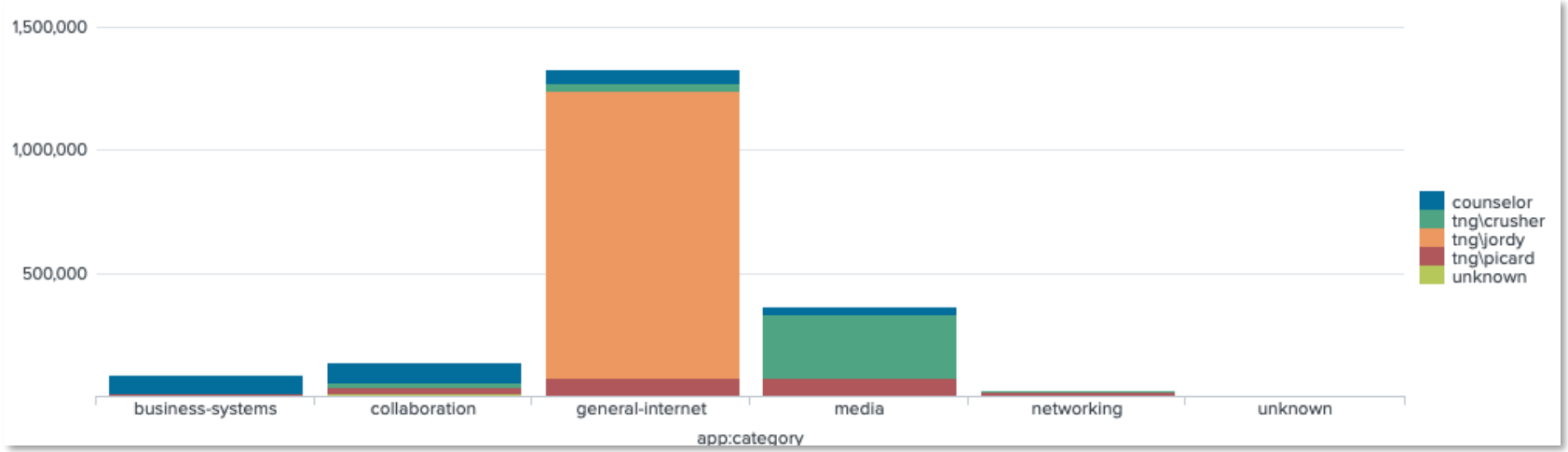


資料結構化chart over欄位 by 欄位

顯示24小時內根據使用者使用應用程式類別分析圖

- 將app:category做事件分組後，各分組使用user在進行事件分類

```
1  sourcetype="pan:traffic"
2  | chart avg(bytes) over app:category by user
```



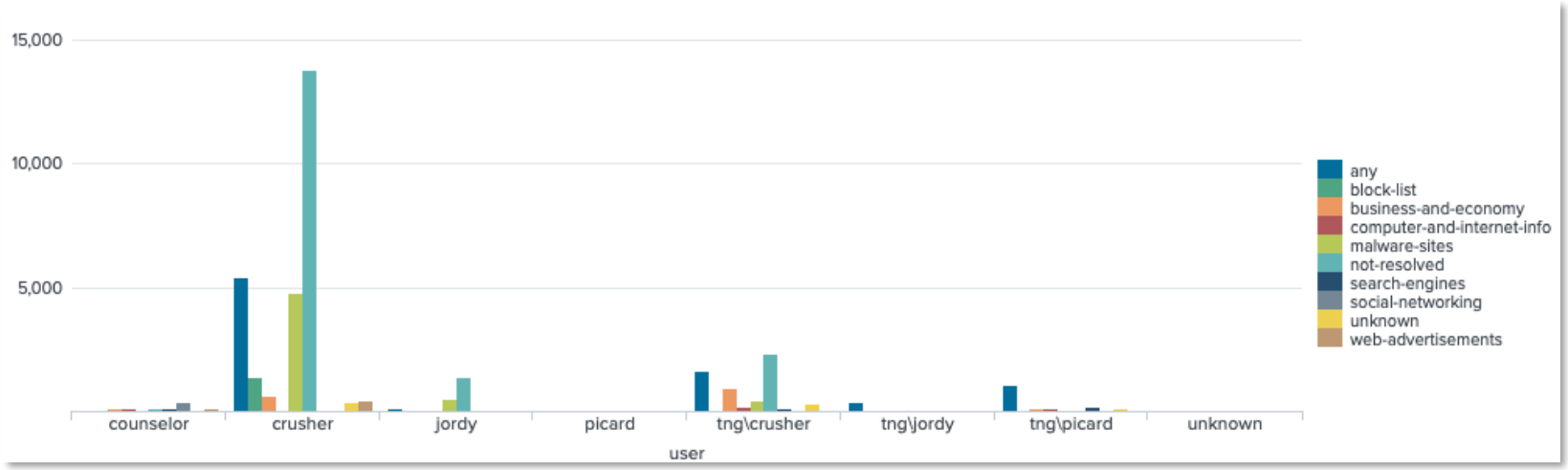
資料結構化chart Null and Other values

程式驅動 code-driven

想看到最近4小時威脅分析大於4的威脅次數，根據各類別及使用者來分析

你會發現圖表裡占比最重的是Null and Other，但這樣的結果並不是我們想看到的

```
1  sourcetype="pan:threat" app:risk>=4
2  | chart usenull=f useother=f count over user by category
```



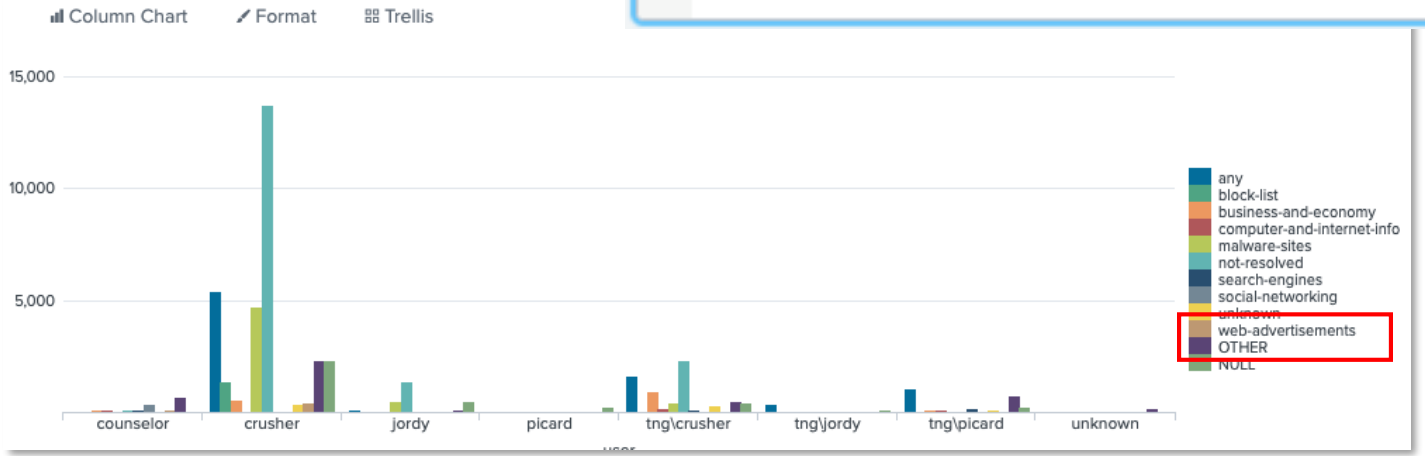
資料結構化chart Null and Other values

程式驅動 code-driven

想看到最近4小時威脅分析大於4的威脅次數，根據各類別及使用者來分析

chart與timechart指令預設過濾結果只取最高值前十名顯示
–剩餘的值會被集中到OTHER
要移除empty(null)可使用usernull=f
要移除OTHER可使用userother=f

```
1  sourcetype="pan:threat" app:risk>=4
2  | chart count over user by category
```

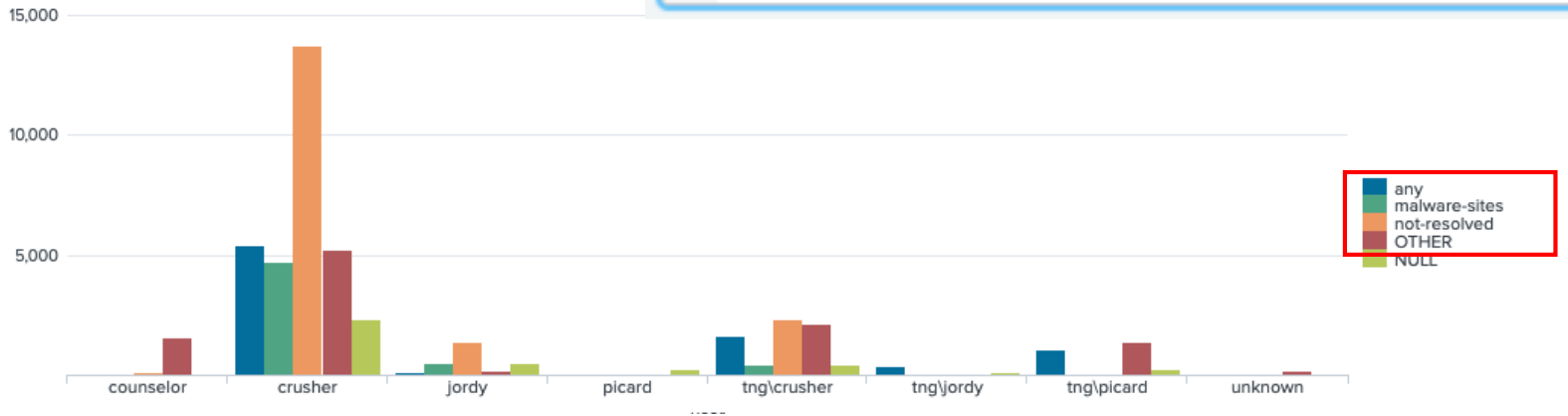


資料結構化chart限制顯示數量

想看到最近4小時威脅分析大於4的威脅次數，根據各類別及使用者來分析

使用limit參數，limit=0為不限制數量

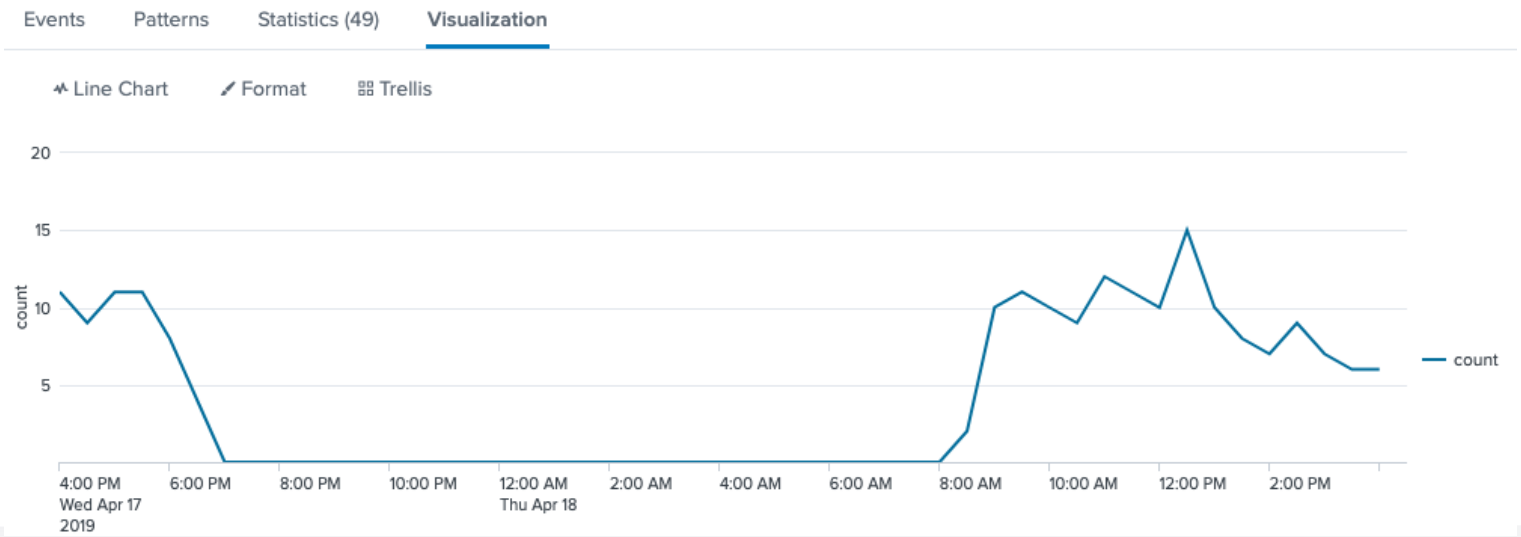
```
1  sourcetype="pan:threat" app:risk>=4
2  | chart count over user by category limit=3
```



時間趨勢圖timechart

想看到24小時內威脅分數為5的趨勢圖

```
1  sourcetype="pan:threat" app:risk>=5
2  | timechart count
```

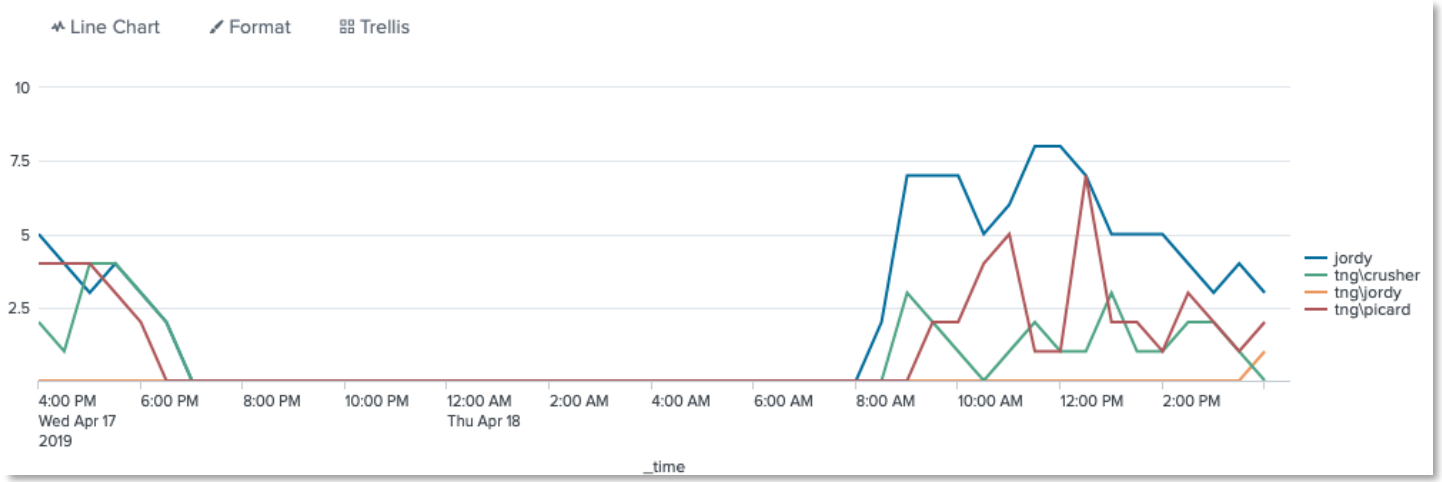


時間趨勢圖timechart

想看到24小時內各使用者威脅分數為5的趨勢分析圖

timechart最多只能選一個欄位作時間群組後的事件分類

```
1  sourcetype="pan:threat" app:risk>=5
2  | timechart count by user
```



時間趨勢圖timechart 調整採樣間隔

程式驅動 code-driven

```
1  sourcetype="pan:threat" app:risk>=4
2  | timechart span=10m count by user
```

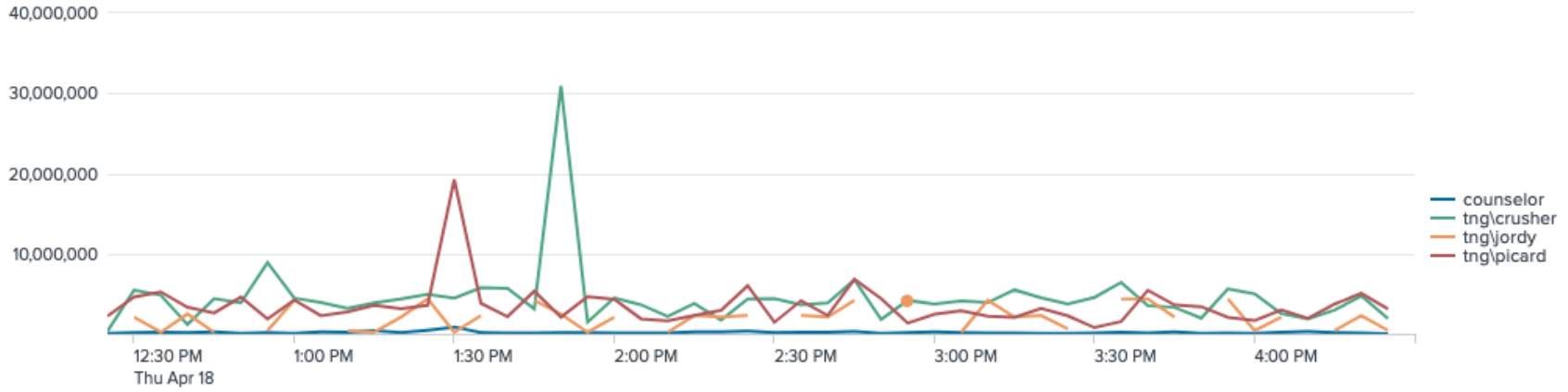
_time	counselor	crusher
2019-04-17 16:00:00	64	1295
2019-04-17 16:10:00	84	1295
2019-04-17 16:20:00	75	1331
2019-04-17 16:30:00	67	1312
2019-04-17 16:40:00	67	1328
2019-04-17 16:50:00	70	1297
2019-04-17 17:00:00	69	1203
2019-04-17 17:10:00	63	1288

- Example defaults:
  - Last 60 minutes uses span=1m
  - Last 24 hours uses span=30m
- Adjust the interval using the span argument, i.e. span=15m

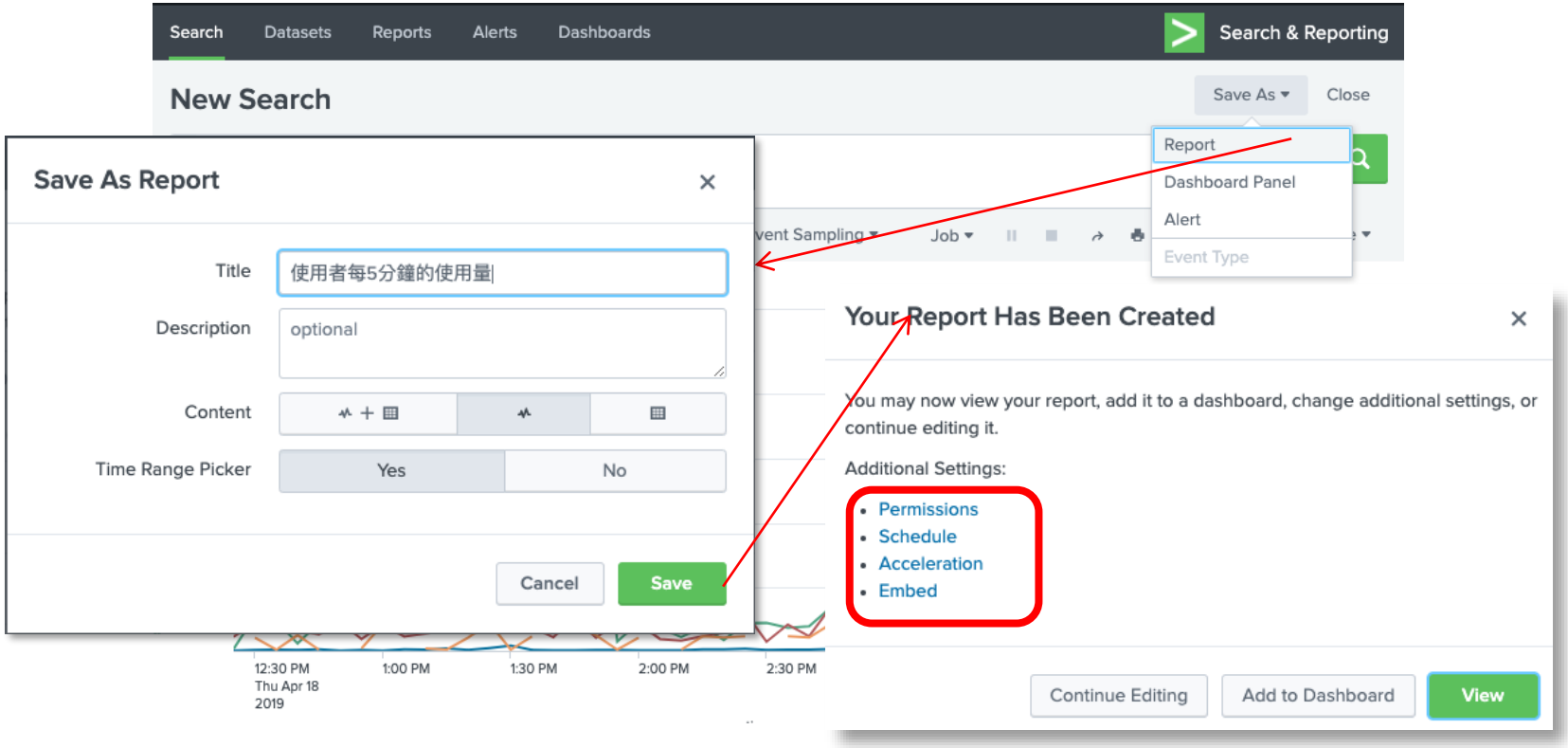
時間趨勢圖timechart 使用統計參數

想看到4小時內從使用者每5分鐘的使用量趨勢分析圖

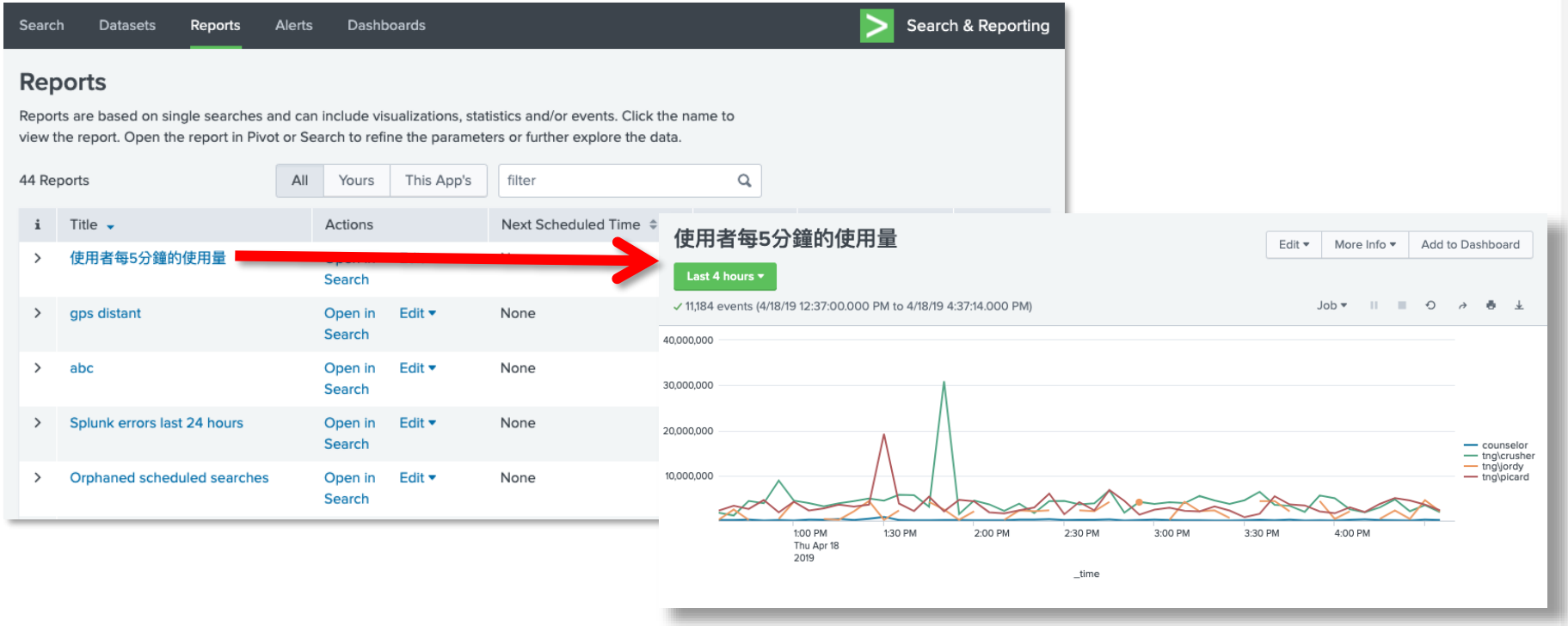
```
1  sourcetype="pan:traffic" app=web*
2  | timechart span=5m sum(bytes) by user
```



另存為『報告』，方便再利用


Search
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Close
Report
Dashboard Panel
Alert
Event Type
Save As Report
Title
使用者每5分鐘的使用量
Description
optional
Content
Time Range Picker
Yes
No
Cancel
Save
Your Report Has Been Created
You may now view your report, add it to a dashboard, change additional settings, or continue editing it.
Additional Settings:
Permissions
Schedule
Acceleration
Embed
Continue Editing
Add to Dashboard
View
12:30 PM
Thu Apr 18
2019
1:00 PM
1:30 PM
2:00 PM
2:30 PM

以後，就可以直接點選搜尋和報告，直接瀏覽

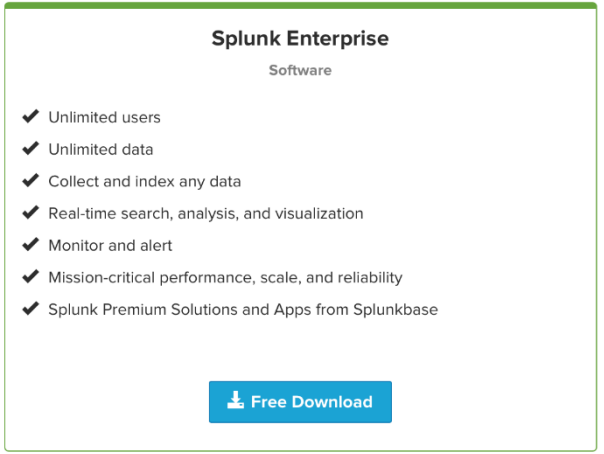


Splunk資源

免費試用

程式驅動 code-driven

- Splunk Enterprise (term)
  - 60 days enterprise full features, then free with limited features
  - 500MB/day
  - Violation = 4 warnings (rolling 30-day period)



探索 Splunk

程式驅動 code-driven

- **Links Referenced in Exploring Splunk**

Chapter	Topic	Description	Link
2	tutorial	The Splunk Tutorial	docs.splunk.com/Documentation/Splunk/4.2/User/WelcometotheSplunktutorial
2	add_data	Tutorial: how to add sample data	docs.splunk.com/Documentation/Splunk/4.2/User/Adddatatutorial
2	sample_data	Tutorial: link to sample data	www.splunk.com/base/images/Tutorial/Sampledata.zip
3	mining_tips	Mining unfamiliar data	www.innovato.com/splunk/mining.htm
5	auto_fields	More information on automatic field extraction	docs.splunk.com/Documentation/Splunk/latest/knowledge/Aboutfields#An_example_of_automatic_field_extraction
5	ifx	More information about the Interactive Field Extractor (IFX)	docs.splunk.com/Documentation/Splunk/4.2/User/InteractiveFieldExtractionExample
5	config_fields	Manually configuring field extractions	docs.splunk.com/Documentation/Splunk/latest/Knowledge/Managesearch-timefieldextractions
5	search_fields	Use the search language to extract fields	docs.splunk.com/Documentation/Splunk/4.2/User/ExtractFieldsWithSearchCommands
5	custom_alerts	Creating custom alert scripts	docs.splunk.com/Documentation/Splunk/4.2/admin/ConfigureScriptedAlerts
6	concurrency	The concurrency search command	docs.splunk.com/Documentation/Splunk/latest/SearchReference/Concurrency
6	metadata	The metadata search command	docs.splunk.com/Documentation/Splunk/latest/SearchReference/metadata
6	streamstats	The streamstats search command	docs.splunk.com/Documentation/Splunk/latest/SearchReference/streamstats
6	trendline	The trendline search command	docs.splunk.com/Documentation/Splunk/latest/SearchReference/Trendline
8	autolookup	Configuring automatic Lookups	docs.splunk.com/Documentation/Splunk/4.2/User/CreateAndConfigureFieldLookups
8	lookuptutorial	Lookup tutorial	docs.splunk.com/Documentation/Splunk/4.2/User/Fieldlookupstutorial

Splunkbase 有2,053個安裝套件(App)，可免費下載安裝

熱門下載：

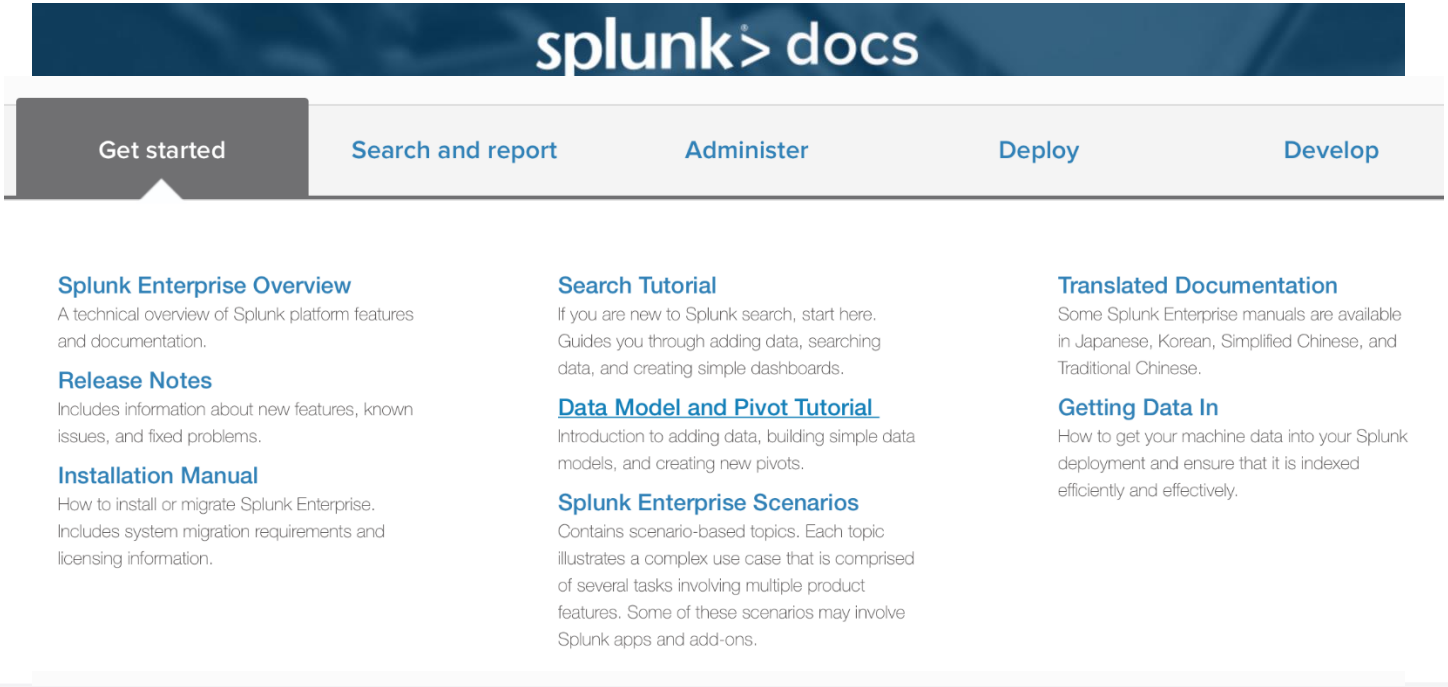
- Splunk App for Windows
- Splunk for Unix and Linux
- DB Collect
- Splunk for Cisco Firewall
- Splunk for F5
- Splunk for Nagios
- Splunk for Web Intelligence
- ..
- ..
- ..

http://apps.splunk.com

相關文件

程式驅動 code-driven

http://docs.splunk.com



研討會、案例、用戶分享

程式驅動 code-driven

- http://conf.splunk.com

.CONF ARCHIVES

2016 Keynotes, Speakers & Sessions

2015 Highlights Video

2015 Sponsors

2015 Keynotes

2015 Speakers & Sessions

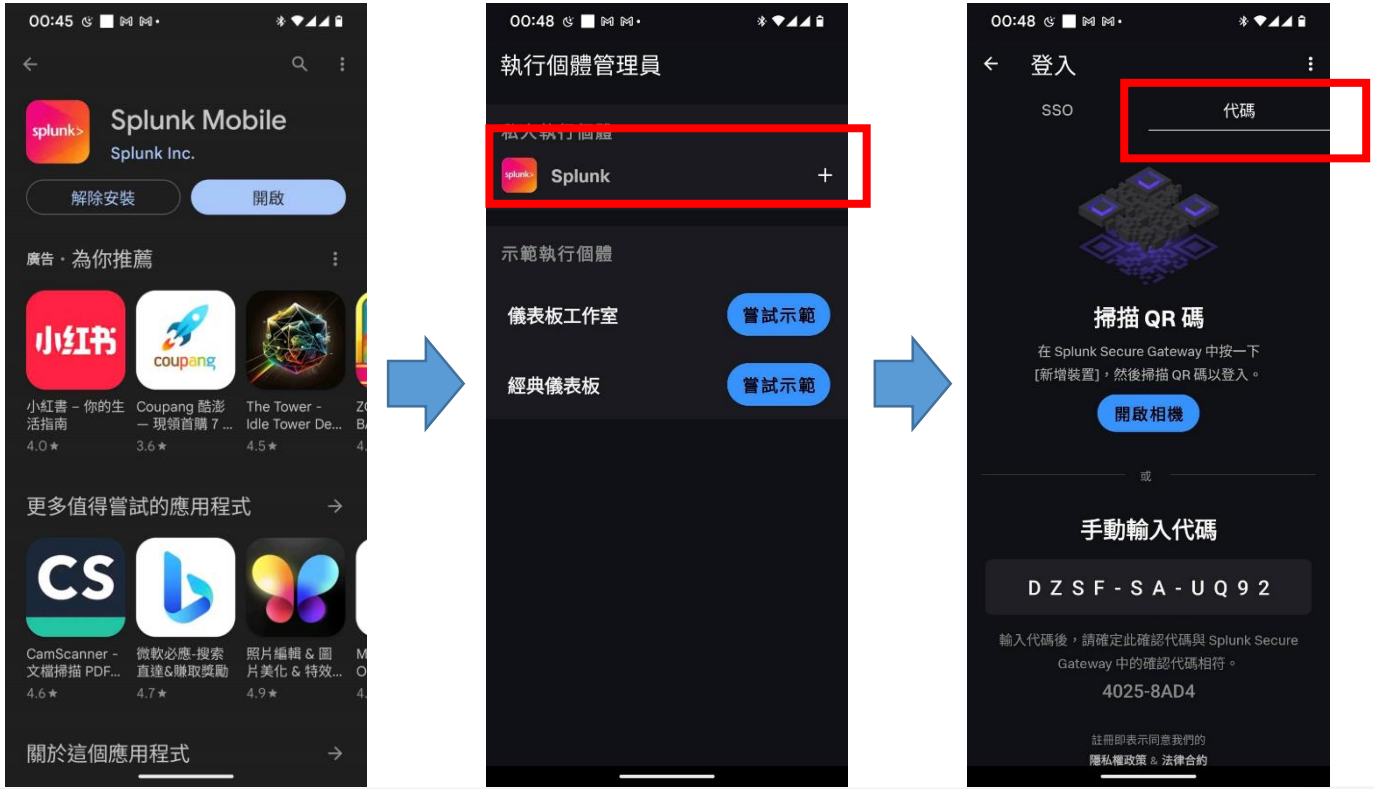
2015 theCube Interviews

2014 Keynotes

2014 Sessions

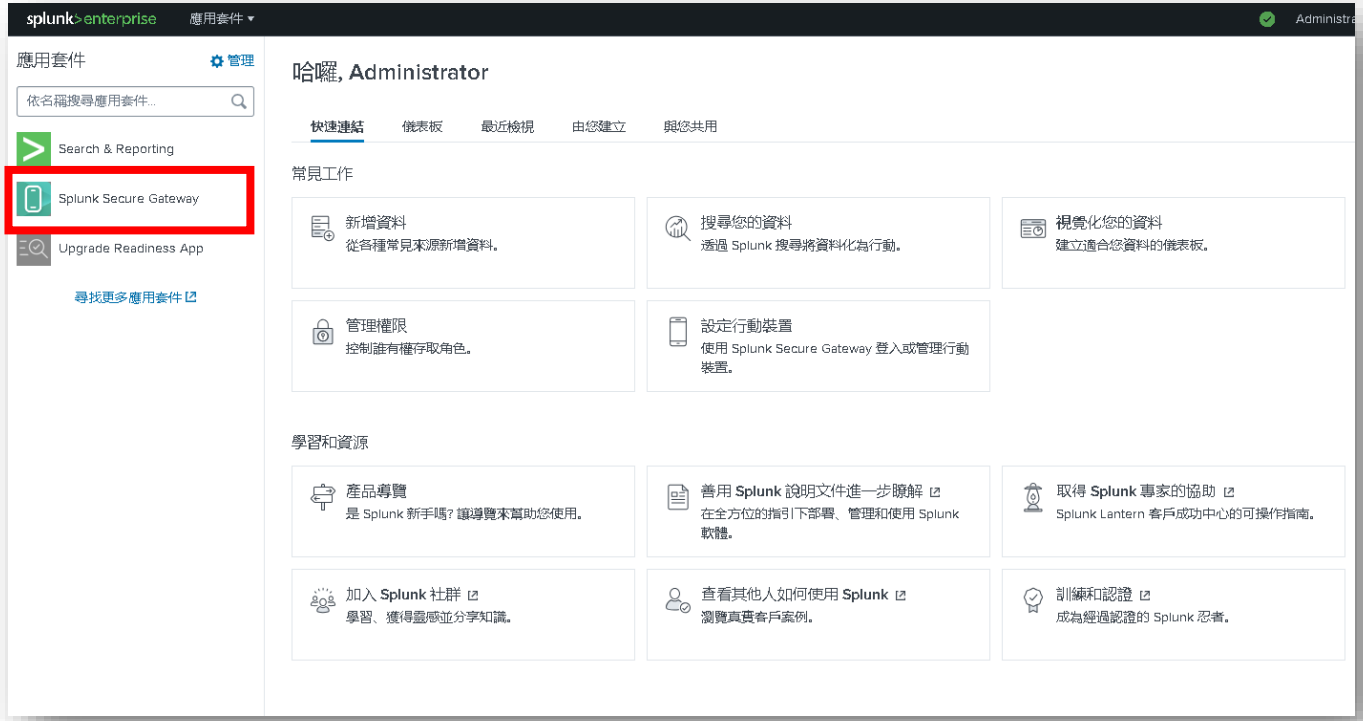
Splunk Secure Gateway

下載 Splunk Mobile

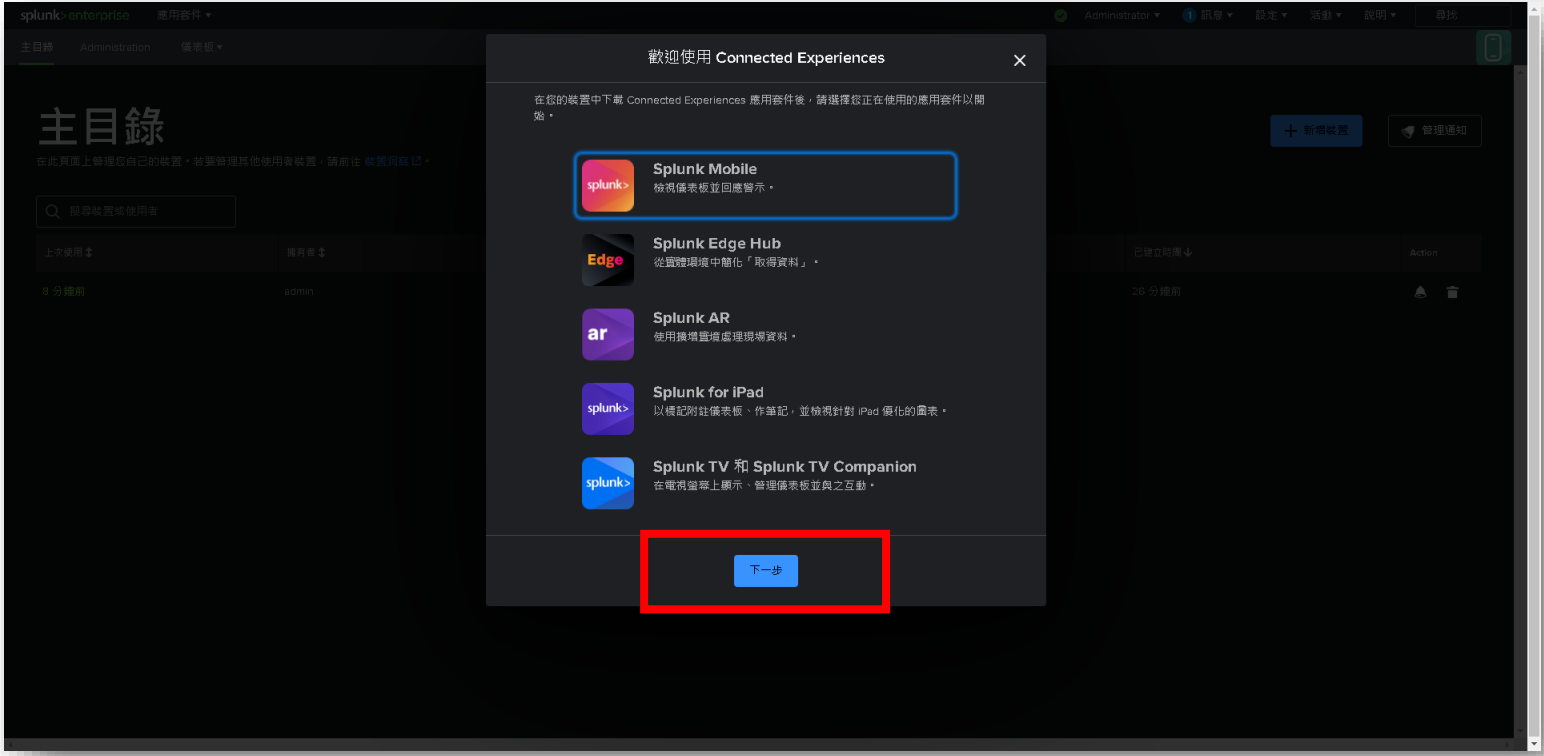


Splunk Secure Gateway

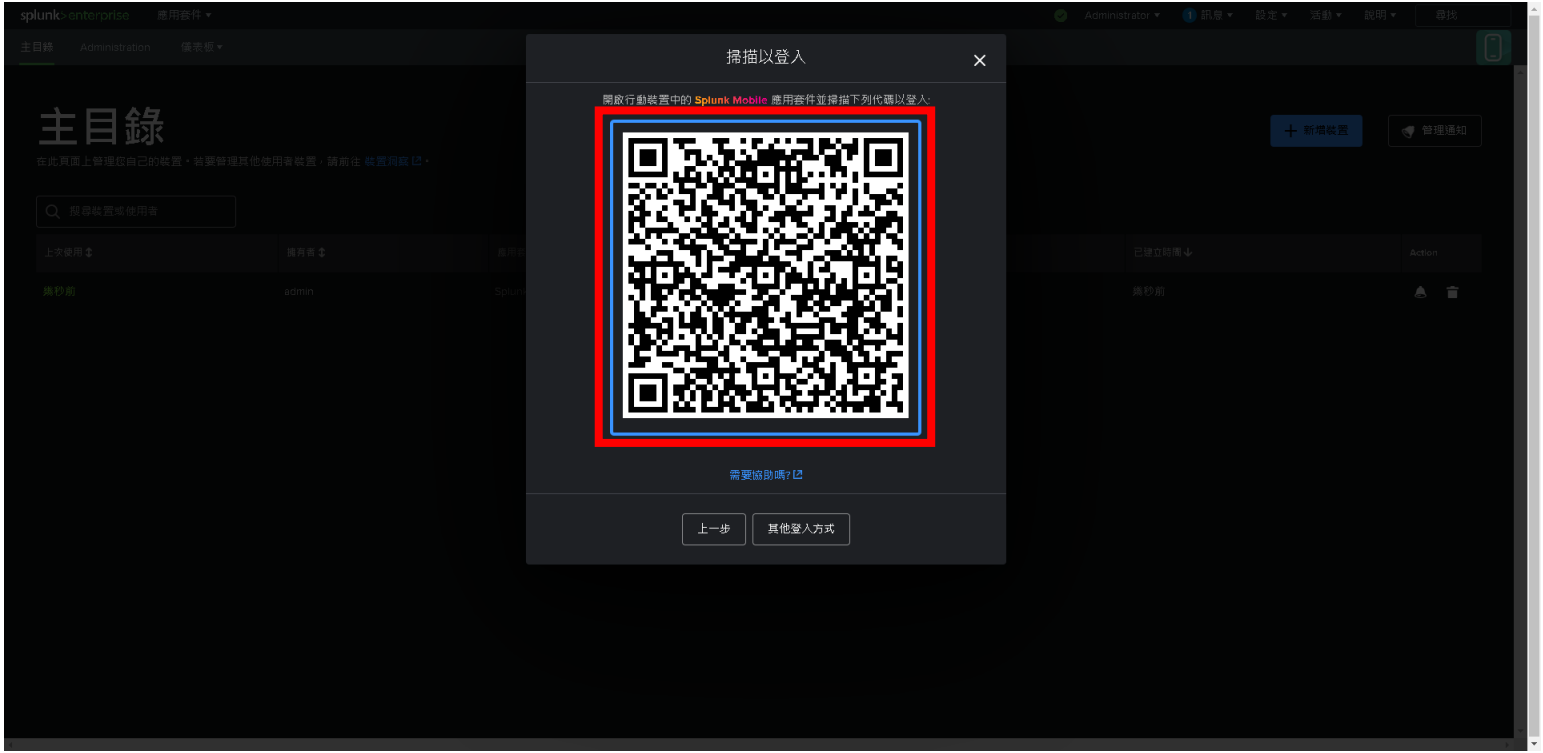
程式驅動 code-driven



Splunk Secure Gateway

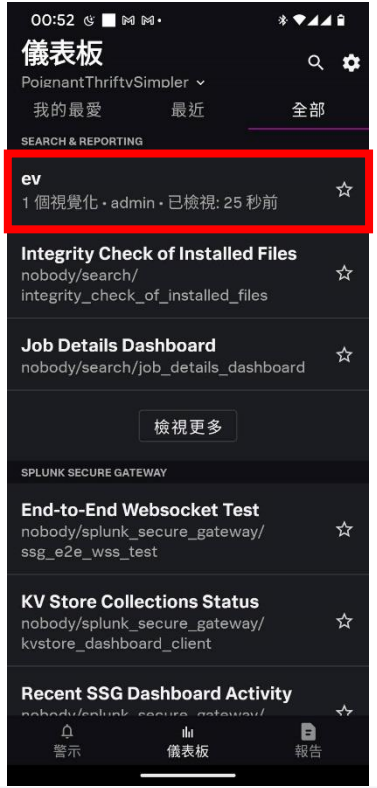


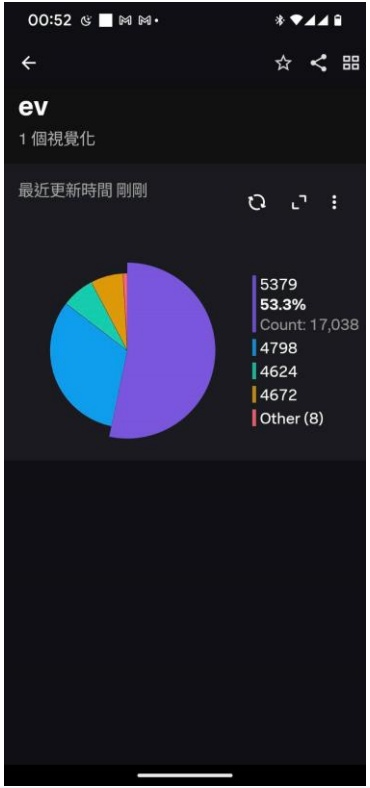
Splunk Secure Gateway



Splunk Secure Gateway

程式驅動 code-driven





Thank you.

程式驅動

code-driven