splunk> 高等教育相關應用案例

教務大數據分析應用分享

Gary Chung
Senior Sales Engineer - Taiwan
http://goo.gl/CRpHt6

Mar 2018

splunk>

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Agenda

Splunk 價值主張

- Splunk **公司簡介**
- Splunk **『 即時維運智慧分析與管理平台』**
- Splunk **校務相關案例分享**

splunk> 公司簡介

公司

舊金山

倫敦 全球總部

香港

全球員工數： **2700+**

年營收： **$932M**

+40%

產品

- 從免費測試到大量佈建
- 產品包含:
  - Splunk Enterprise
  - Splunk Cloud
  - Hunk
  - Premium Solutions
    - **ITSI**
    - **Enterprise Security**
    - **UBA**

客戶

全球客戶數 **14,000+**

台灣客戶數 **400+**

90+ 財星百大企業

20+ 標準非結構資料平台

最大用戶：

3000+ Terabytes/日

願景：機器資料(Machine Data) 彙集、**搜尋**及即時分析引擎

使每個人能 **快速** 取得、使用機器資料並 **產生價值**.

全球超過 14,000 個客戶應用

雲端、線上服務

salesforce, white pages, LinkedIn, facebook, edmunds.com, Concur, RightNow, PayPal, StubHub!, ebay, HOOVERS A D&B COMPANY

教育機構

MICHIGAN, Ucla, University of Maryland, Cal, TEXAS, Stanford, GW, Washington State University, Penn State, University of Connecticut, USC TROJANS

能源與公共事業

Schlumberger, ALLIANT ENERGY, ULTRA PETROLEUM, ENBRIDGE, pjm, SOUTHERN CALIFORNIA EDISON An EDISON INTERNATIONAL Company, California ISO Shaping a Renewed Future, noble energy, TOTAL, urenco

金融保險業

WELLS FARGO, Bank of America, NEW YORK LIFE, CREDIT SUISSE, fiserv., Aetna, Morgan Stanley, VISA, COMMERZBANK

政府機關

U.S. Department of the Interior Bureau of Land Management, Department of Defense, United States Marine Corps, USAID FROM THE AMERICAN PEOPLE, Department of Energy, United States Navy, SOCOM, U.S. ARMY, City of Phoenix, Department of Homeland Security, U.S. AIR FORCE

醫療照護產業

UCLA Health System, H, COVIDIEN, Health Net, HEALTHSPRING, HEALTHTRANS, Children's Mercy HOSPITALS & CLINICS www.childrensmercy.org, ST. JUDE MEDICAL, MCKESSON, COVENTRY Health Care, medco

製造業

Raytheon, LOCKHEED MARTIN, PPG, adidas, PEPSICO, NORTHROP GRUMMAN, Pitney Bowes, Snap-on, GENERAL DYNAMICS

媒體與娛樂產業

BBC, DOW JONES, wp Washington Post Media, DIRECTV SATELLITE TELEVISION, SONY, GANNETT, audience network, Discovery COMMUNICATIONS, NATIONAL GEOGRAPHIC, comcast

零售業

LOWE'S, CVS CAREMARK, otto group, RESTORATION HARDWARE, jcpenney, STAPLES, GILT GROUPE, WILLIAMS-SONOMA, WAL★MART

高科技業

IBM, CITRIX, EMC², vmware, TREND MICRO, Adobe, intuit, Symantec, cisco, QUALCOMM, Autodesk

電信業

metroPCS, SaskTel, Time Warner Cable, T-Mobile, at&t, Telstra, HughesNet, vodafone, MOTOROLA, swisscom

旅遊與休閒產業

VEGAS.com, Pegasus SOLUTIONS, TOLL, carlson marketing, INTERVAL INTERNATIONAL THE QUALITY VACATION EXCHANGE NETWORK, ORBITZ, ACCOR, HomeAway, sun country airlines

splunk> listen to your data

超過 450 所教育機構採用

THE UNIVERSITY OF TEXAS AT AUSTIN
Georgia Tech
AUBURN
WINONA STATE UNIVERSITY
NORTH CAROLINA STATE UNIVERSITY
CORNELL UNIVERSITY
WASHINGTON STATE UNIVERSITY
LSU
Portland State UNIVERSITY
MichiganTech
上海交通大學 Shanghai Jiao Tong University
UNIVERSITY OF MARYLAND
THE STATE UNIVERSITY OF NEW JERSEY RUTGERS
UCLA
Sheridan
COLLEGE of CHARLESTON
THE UNIVERSITY OF UTAH
KU THE UNIVERSITY OF KANSAS
UNIVERSITY OF HOUSTON Learning. Leading.
GEORGETOWN UNIVERSITY
LA TROBE UNIVERSITY
USC UNIVERSITY OF SOUTHERN CALIFORNIA
UNIVERSITY OF MICHIGAN
SONOMA STATE UNIVERSITY
THE UNIVERSITY of ADELAIDE
RU RADFORD UNIVERSITY
The Open University
國立交通大學 National Chiao Tung University
MUSC MEDICAL UNIVERSITY of SOUTH CAROLINA
WestVirginiaUniversity
THE UNIVERSITY OF MELBOURNE
國立中央大學
UNIVERSITY AT ALBANY State University of New York
Mc Graw Hill
CENTRAL WASHINGTON UNIVERSITY Your future is Central.
UTSA University of Texas at San Antonio
THE GEORGE WASHINGTON UNIVERSITY WASHINGTON DC
Drexel UNIVERSITY
MIAMI UNIVERSITY OXFORD OHIO
NANYANG TECHNOLOGICAL UNIVERSITY
The University of Georgia
SYRACUSE UNIVERSITY FOUNDED A.D. 1870
CALIFORNIA STATE UNIVERSITY LONG BEACH
YORK COLLEGE The City University of New York
國立高雄第一科技大學 National Kaohsiung First University of Science and Technology
University of Connecticut
Kun Shan University 崑山科技大學
THE UNIVERSITY OF SCRANTON A JESUIT UNIVERSITY
MiraCosta College
THE UNIVERSITY OF CALIFORNIA 1868
KENT STATE UNIVERSITY
FLORIDA STATE UNIVERSITY 1851
SUNGARD HIGHER EDUCATION
CALIFORNIA STATE UNIVERSITY Chico

splunk> listen to your data

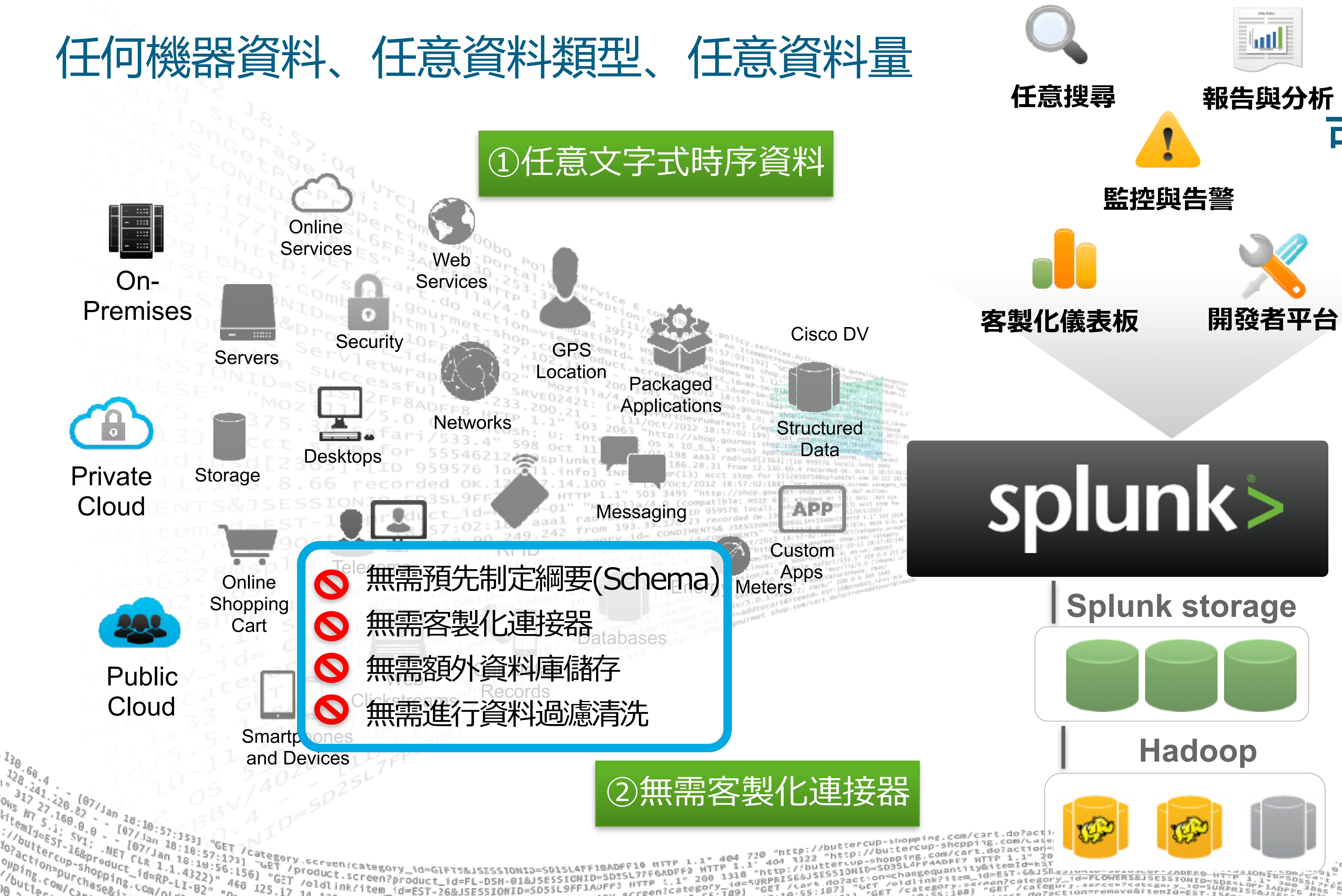
Agenda

Splunk 價值主張

- Splunk **公司簡介**
- Splunk『 **即時維運智慧分析與管理平台**』
- Splunk **校務相關案例分享**

將任意資料轉換成價值

任何機器資料、任意資料類型、任意資料量



①任意文字式時序資料

- 無需預先制定綱要(Schema)
- 無需客製化連接器
- 無需額外資料庫儲存
- 無需進行資料過濾清洗

②無需客製化連接器

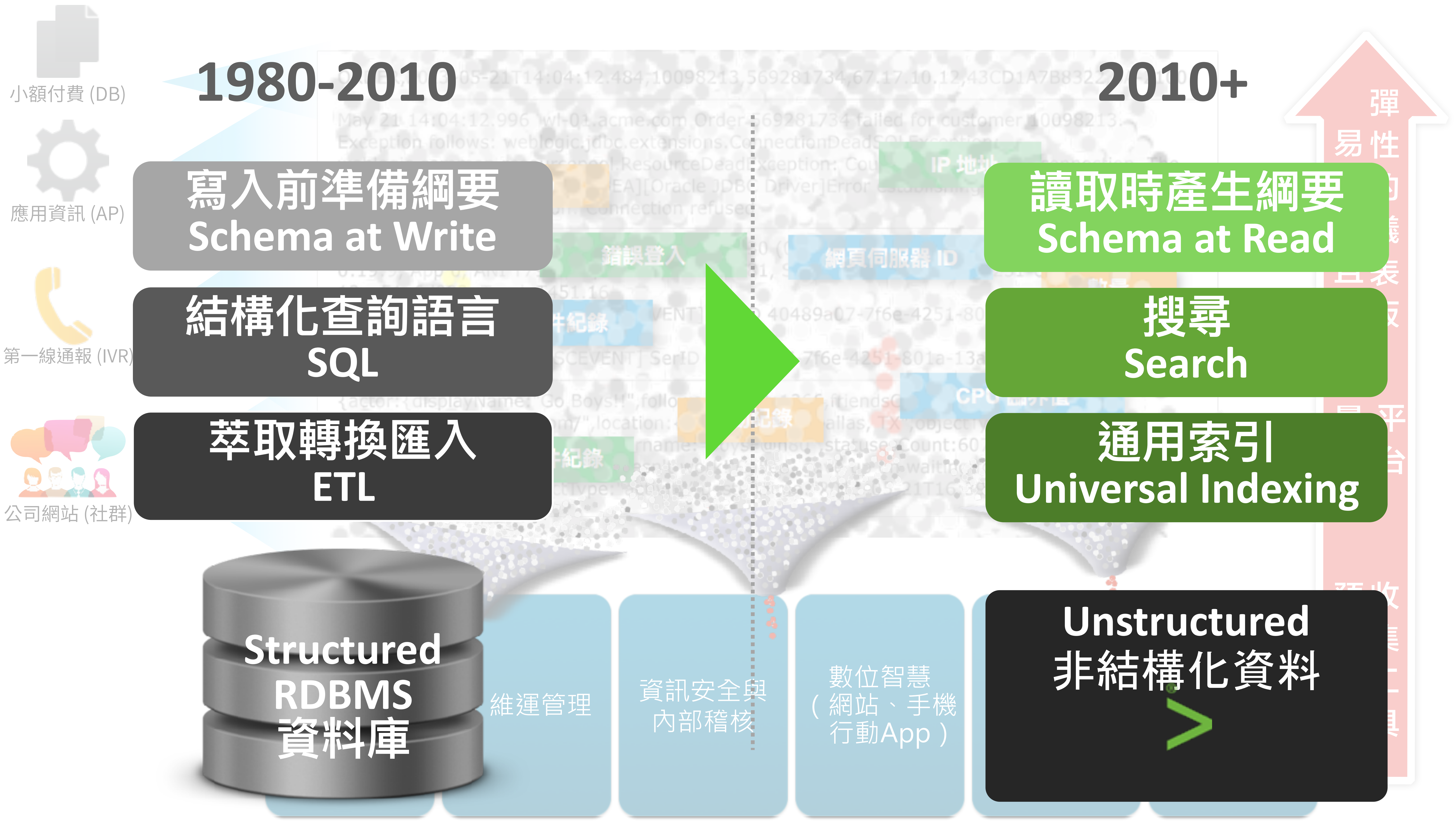
③ 高速**即時**搜尋以及預測數值/分析異常

可針對資料問任意問題

- 應用程式派送
- IT 維運管理
- 資訊安全，防詐欺等
- 商業(校務)分析
- 物聯網資料分析

splunk> listen to your data

全資料帶來的各種可延伸性



1980-2010

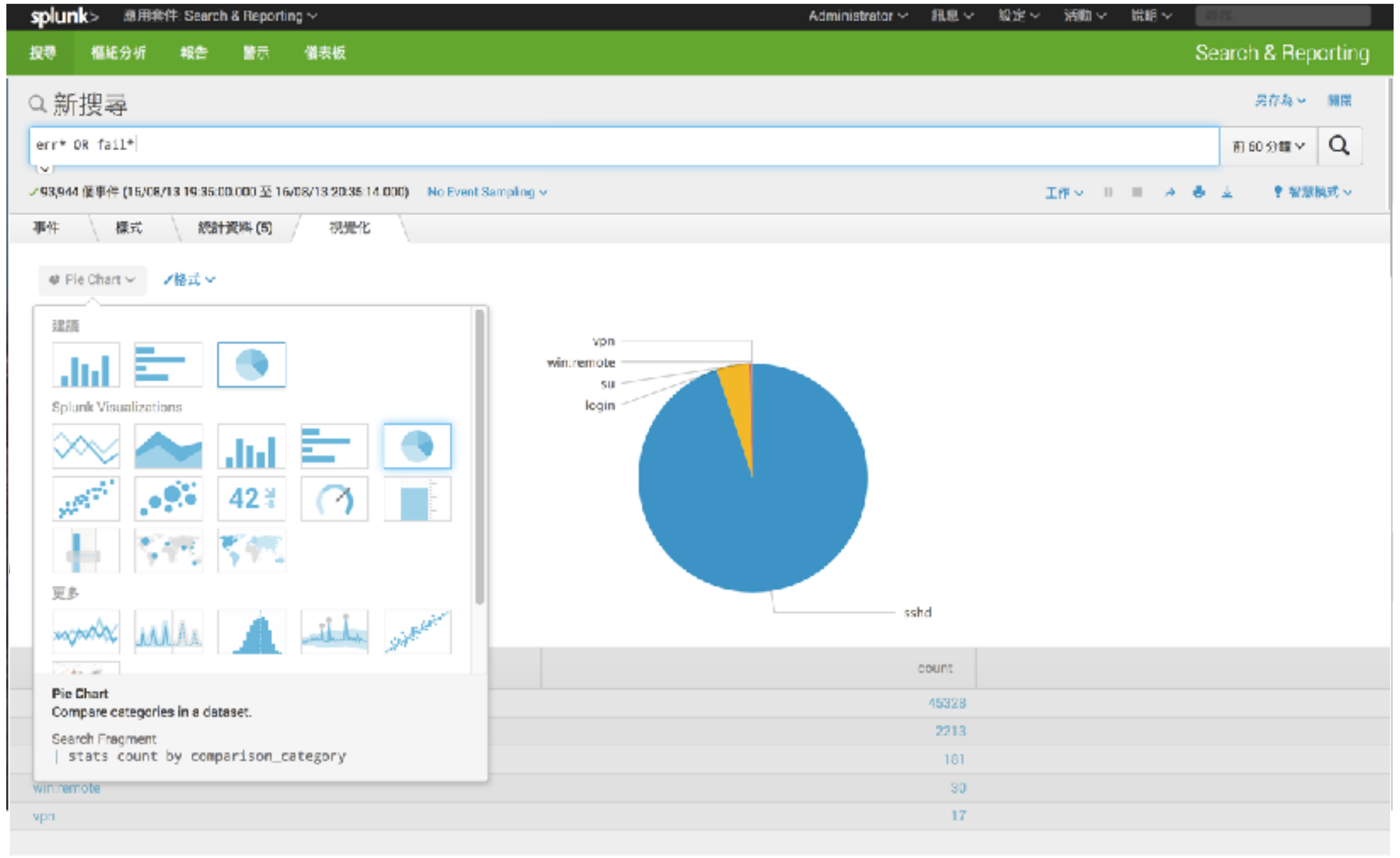
- 寫入前準備綱要 Schema at Write
- 結構化查詢語言 SQL
- 萃取轉換匯入 ETL
- Structured RDBMS 資料庫

2010+

- 讀取時產生綱要 Schema at Read
- 搜尋 Search
- 通用索引 Universal Indexing
- Unstructured 非結構化資料

從不同方式找尋問題點

像 Google 一樣以分散式方法尋找問題



```
err* OR fail*
```

✓93,944 個事件 (15/08/13 19:35:00.000 至 16/08/13 20:35:14.000) No Event Sampling

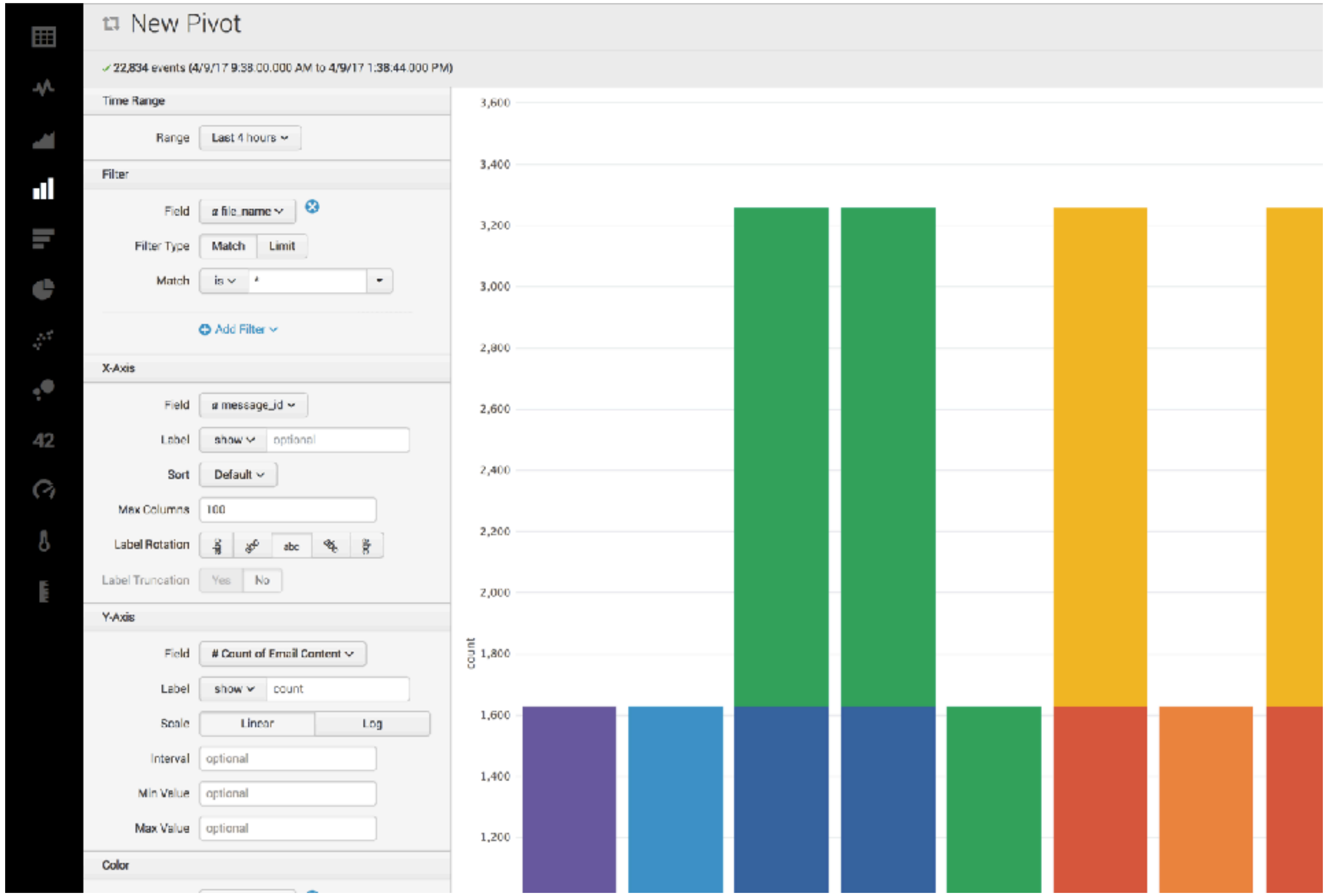
Pie Chart
Compare categories in a dataset.

Search Fragment

```
| stats count by comparison_category
```

	count
	45328
	2213
	161
win:remote	30
vpn	17

像 BI 工具一樣挖掘洞察力



New Pivot

✓22,834 events (4/9/17 9:38:00.000 AM to 4/9/17 1:38:44.000 PM)

Time Range
Range: Last 4 hours

Filter
Field: a file_name
Filter Type: Match | Limit
Match: is *
Add Filter

X-Axis
Field: a message_id
Label: show | optional
Sort: Default
Max Columns: 100
Label Rotation: abc
Label Truncation: Yes | No

Y-Axis
Field: # Count of Email Content
Label: show | count
Scale: Linear | Log
Interval: optional
Min Value: optional
Max Value: optional

Color

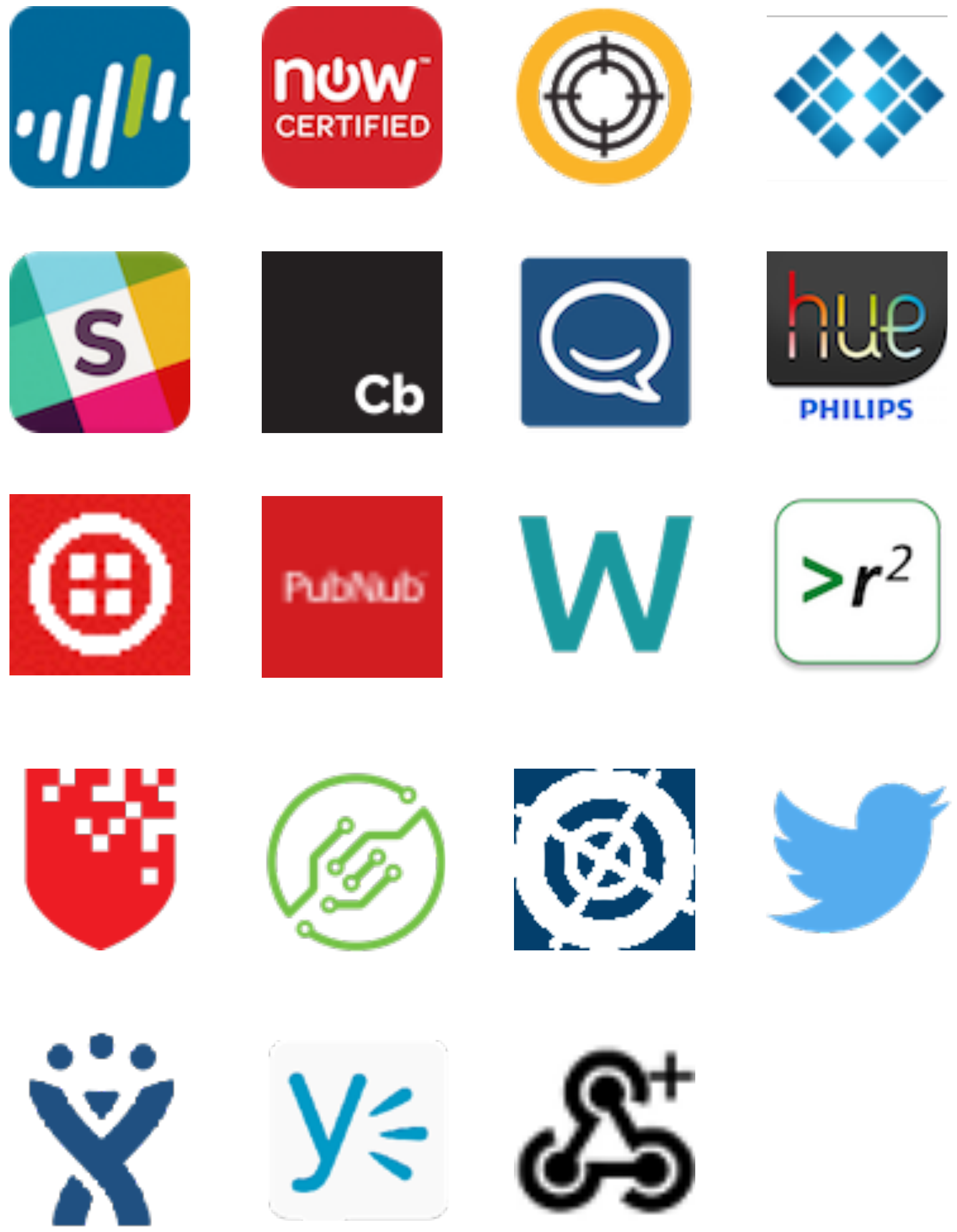
splunk> listen to your data®

彈性化安裝插件的 Splunk 7.0

輸入插件

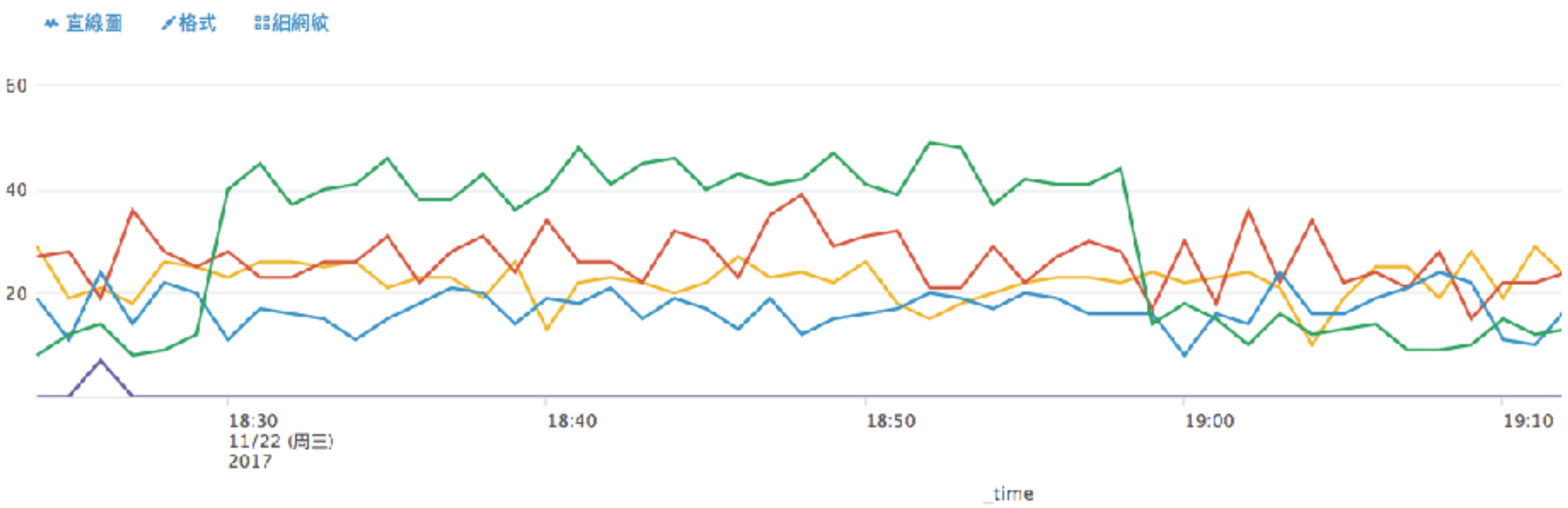
FTP
bing
salesforce
DBX
STM
DELLEMC ISILON
EX
DELLEMC VMAX
okta
f5
ALEXA
Google Cloud Platform
JMS
JMX
WAS
KAFKA
box
MQTT
AMQP
NetApp
SNMP
FBTX

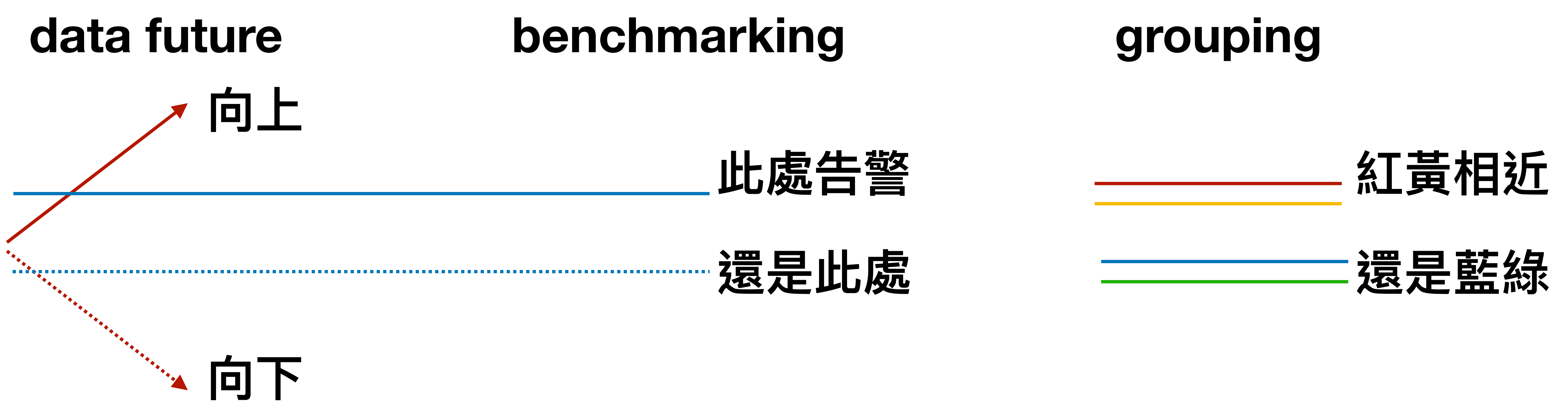
告警插件

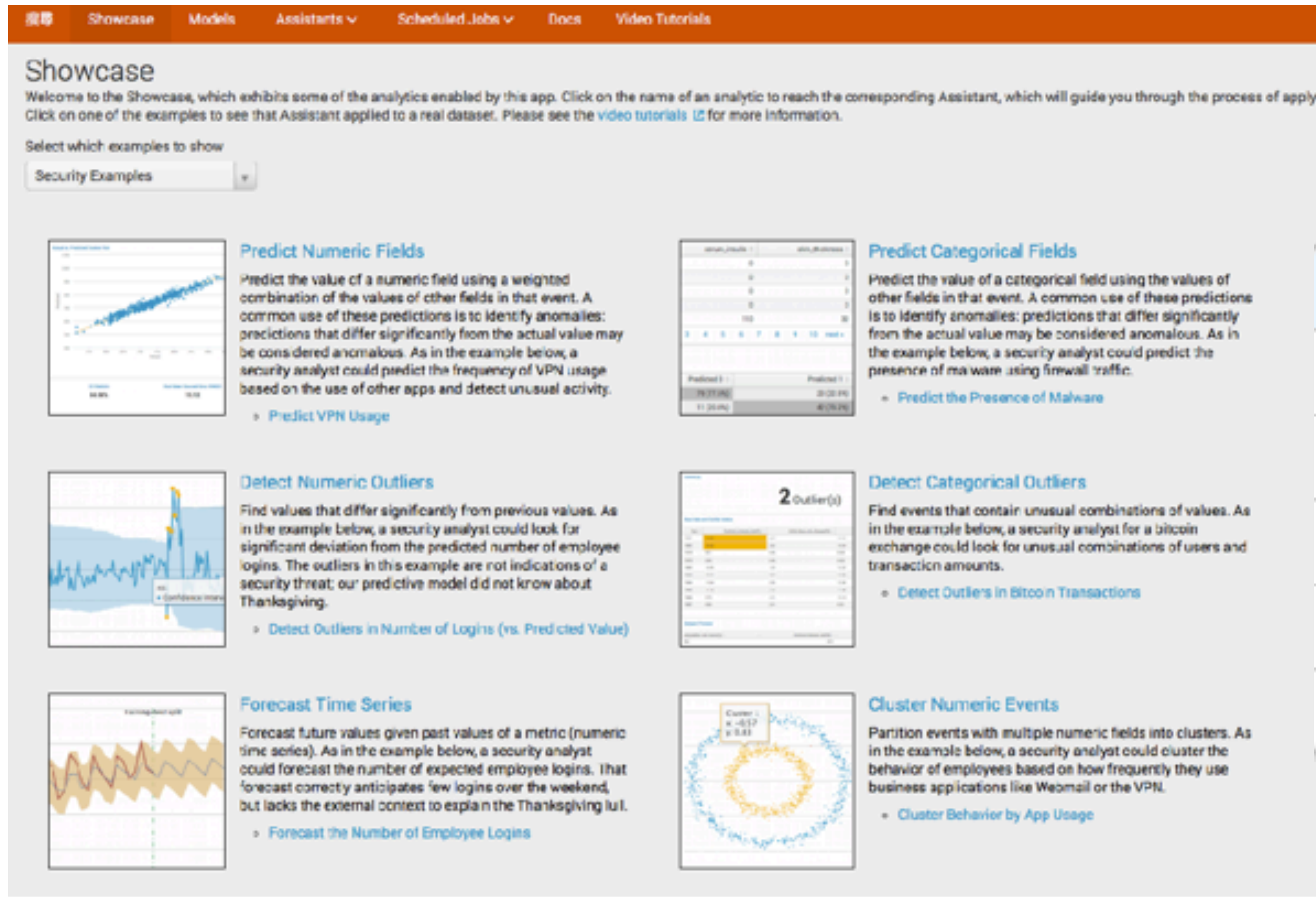


視覺插件

大數據 + 機器學習 = AIOps







Showcase

Welcome to the Showcase, which exhibits some of the analytics enabled by this app. Click on the name of an analytic to reach the corresponding Assistant, which will guide you through the process of applying it to your data. Click on one of the examples to see that Assistant applied to a real dataset. Please see the video tutorials for more information.

Select which examples to show

Security Examples

Predict Numeric Fields

Predict the value of a numeric field using a weighted combination of the values of other fields in that event. A common use of these predictions is to identify anomalies: predictions that differ significantly from the actual value may be considered anomalous. As in the example below, a security analyst could predict the frequency of VPN usage based on the use of other apps and detect unusual activity.

- Predict VPN Usage

Predict Categorical Fields

Predict the value of a categorical field using the values of other fields in that event. A common use of these predictions is to identify anomalies: predictions that differ significantly from the actual value may be considered anomalous. As in the example below, a security analyst could predict the presence of malware using firewall traffic.

- Predict the Presence of Malware

Detect Numeric Outliers

Find values that differ significantly from previous values. As in the example below, a security analyst could look for significant deviation from the predicted number of employee logins. The outliers in this example are not indications of a security threat; our predictive model did not know about Thanksgiving.

- Detect Outliers in Number of Logins (vs. Predicted Value)

Detect Categorical Outliers

Find events that contain unusual combinations of values. As in the example below, a security analyst for a bitcoin exchange could look for unusual combinations of users and transaction amounts.

- Detect Outliers in Bitcoin Transactions

Forecast Time Series

Forecast future values given past values of a metric (numeric time series). As in the example below, a security analyst could forecast the number of expected employee logins. That forecast correctly anticipates few logins over the weekend, but lacks the external context to explain the Thanksgiving lull.

- Forecast the Number of Employee Logins

Cluster Numeric Events

Partition events with multiple numeric fields into clusters. As in the example below, a security analyst could cluster the behavior of employees based on how frequently they use business applications like Webmail or the VPN.

- Cluster Behavior by App Usage

Predict Numeric Fields

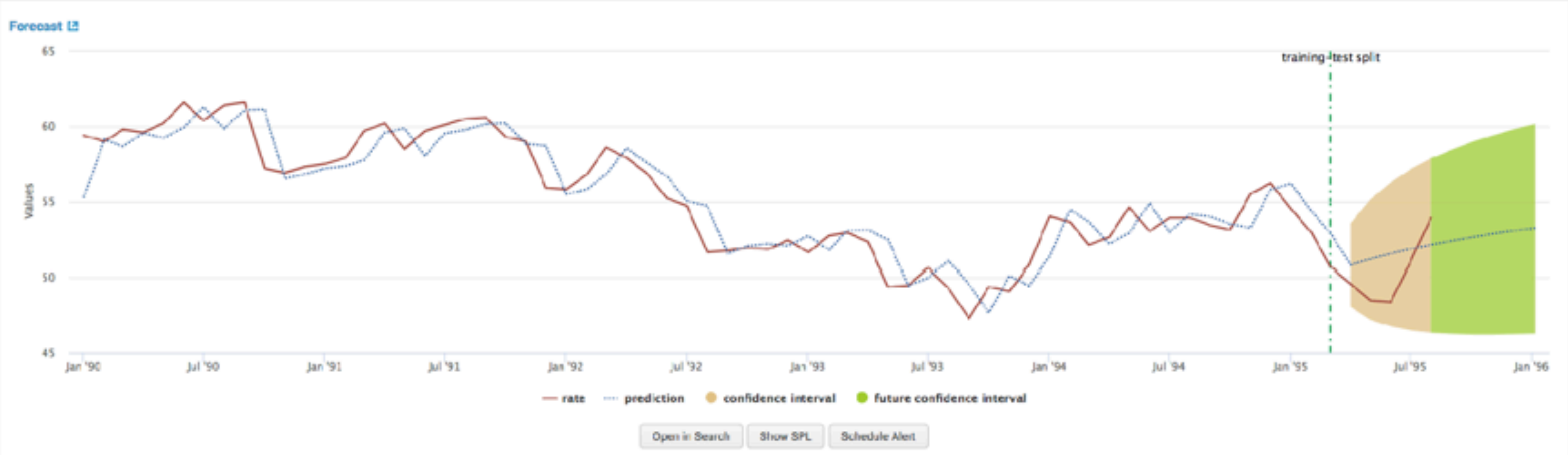
Predict Categorical Fields

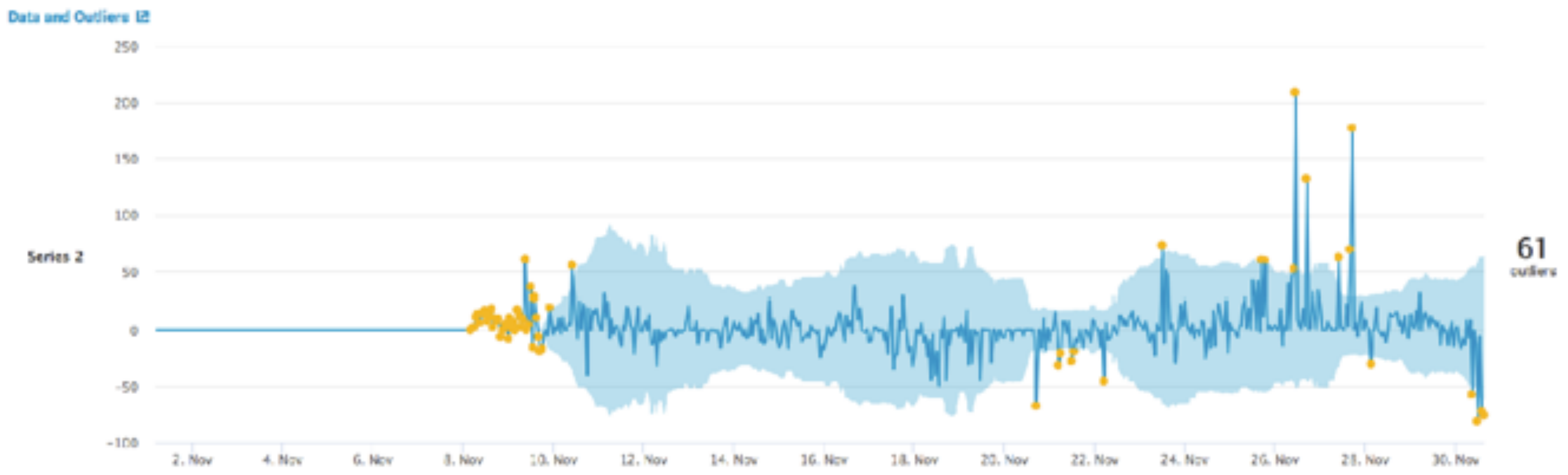
Detect Numeric Outliers

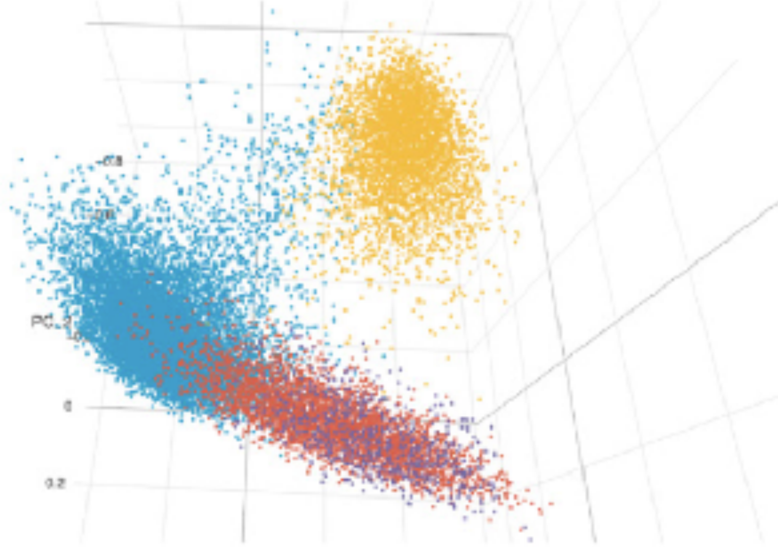
Detect Categorical Outliers

Forecast Time Series

Cluster Numeric Events







不同應用面向的產品

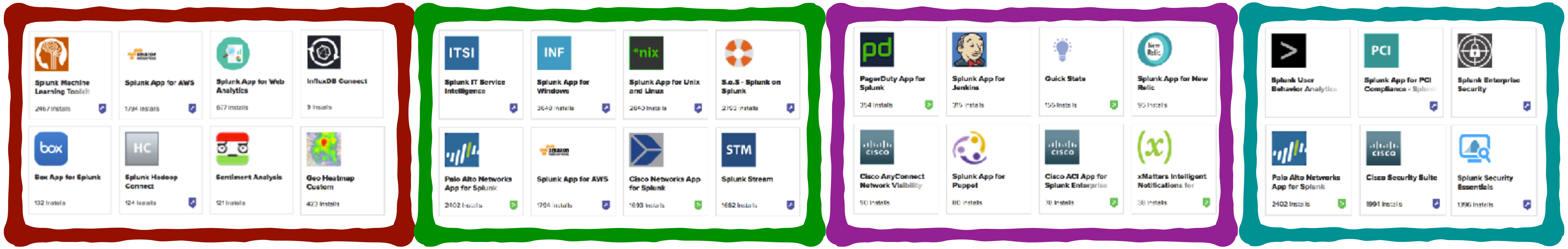
Splunk 進階加值解決方案

- Splunk IT Service Intelligence™
- Splunk Enterprise Security™
- Splunk User Behavior Analytics™

Splunk 針對各種 Insight 方案

- Splunk Security Essentials
- Splunk Security Essentials for Ransomware
- Splunk Security Essentials for Fraud

> 1,500 個應用套件



Splunk Machine Learning Toolkit
2467 Installs

Splunk App for AWS
1794 Installs

Splunk App for Web Analytics
677 Installs

InfluxDB Connect
9 Installs

Box App for Splunk
132 Installs

Splunk Hadoop Connect
124 Installs

Sentiment Analysis
121 Installs

Geo Heatmap Custom
423 Installs

Splunk IT Service Intelligence

Splunk App for Windows
3649 Installs

Splunk App for Unix and Linux
2840 Installs

S.o.S - Splunk on Splunk
2793 Installs

Palo Alto Networks App for Splunk
2402 Installs

Splunk App for AWS
1794 Installs

Cisco Networks App for Splunk
1693 Installs

Splunk Stream
1662 Installs

PagerDuty App for Splunk
354 Installs

Splunk App for Jenkins
315 Installs

Quick Stats
155 Installs

Splunk App for New Relic
95 Installs

Cisco AnyConnect Network Visibility
90 Installs

Splunk App for Puppet
80 Installs

Cisco ACI App for Splunk Enterprise
78 Installs

xMatters Intelligent Notifications for
38 Installs

Splunk User Behavior Analytics

Splunk App for PCI Compliance - Splunk

Splunk Enterprise Security

Palo Alto Networks App for Splunk
2402 Installs

Cisco Security Suite
1991 Installs

Splunk Security Essentials
1396 Installs

splunk>enterprise

splunk>cloud™

splunk> Platform for Operational Intelligence

- Forwarders
- Syslog/ TCP
- Mobile
- IoT Devices
- Network Wire Data
- Hadoop
- Relational Databases
- Mainframe Data

splunk> listen to your data®

Splunk 校務應用洞察

單一平台應用在各種資料產生的綜效

結構資料佔比下降 **行為分析更重視非結構資料**

- 研究計畫
- 教育經驗
- 倫理規範遵守
- 資源最佳化

splunk>

代表性流程

- 招生/學籍管理
- 數位出版
- 教室資源管理
- 電腦運算資源管理
- 使用者計費
- 服務支援中心
- 實驗室資源配置
- 電路資源管理
- 網路管理
- 資訊安全與合規

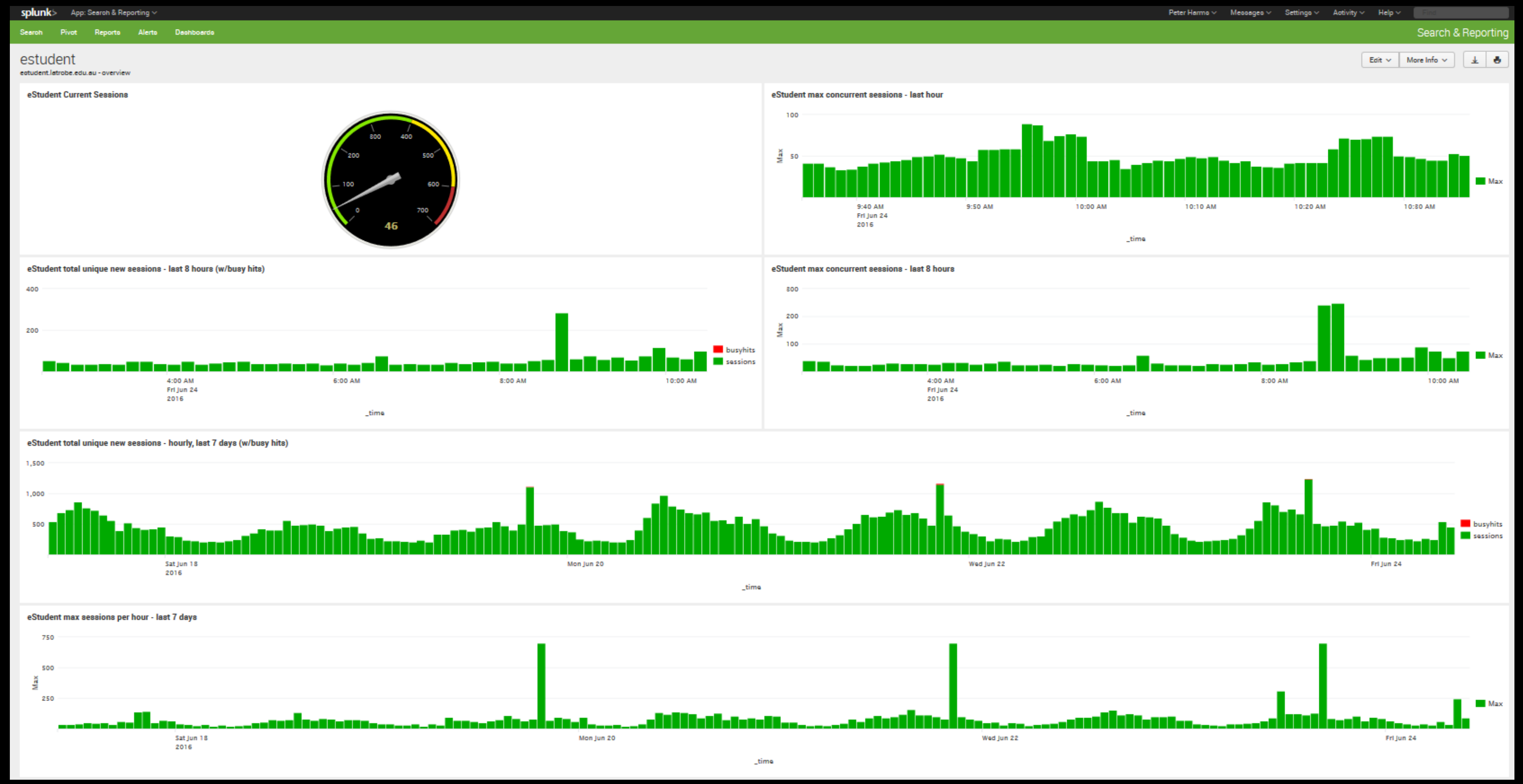
校園服務

- 研究所佔用電腦資源
- 學生註冊
- 學習管理系統
- 遠距學習
- 服務支援中心
- 外部連線 VPN

EDUCATION – ITOA OPERATIONS

解決 IT 問題
進一步讓校務問題變成研究方向

- 徹底解決 Student One 考試成績查詢系統長期(長達兩年找不到根本原因) **系統錯誤**問題
- 將困擾一年多因**學校網域名掉進郵件黑名單**問題而出現的郵件服務中斷問題減少超過90%
- 調查因下載而出現**網絡擁塞**的時間加快 90%，提高管理人員效率1倍
- 簡化和提高調查**無線網路驗證問題**和系統效能的透明度
- 追蹤**無線網路與學生表現**連結



estudent

estudent.latrobe.edu.au - overview

eStudent Current Sessions

eStudent max concurrent sessions - last hour

eStudent total unique new sessions - last 8 hours (w/busy hits)

eStudent max concurrent sessions - last 8 hours

eStudent total unique new sessions - hourly, last 7 days (w/busy hits)

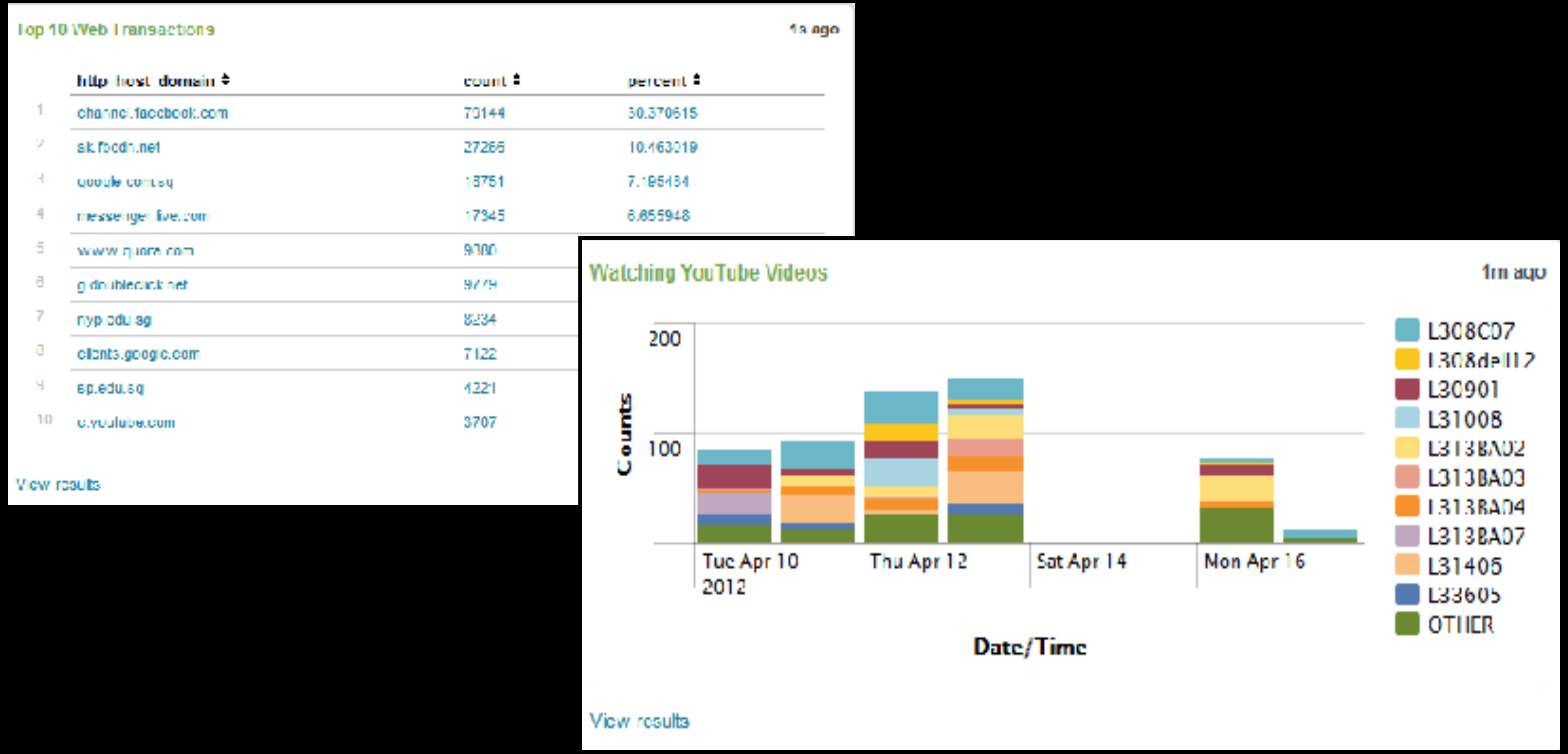
eStudent max sessions per hour - last 7 days

NYP
NANYANG
POLYTECHNIC

EDUCATION – SCHOOL LEVEL ADOPTION

完整校園資源整合應用案例

- 2011 年起建立大數據訓練中心
- 學生社交網路追蹤, 即時課堂評價動態分析
- 開發金融資訊、ＢＩ、ＳＯＣ、ＩＯＴ相關套件
- 學生/校外上網記錄分析



Top 10 Web Transactions

1s ago

	http_host_domain ⇕	count ⇕	percent ⇕
1	channel.facebook.com	79144	30.370615
2	sk.fbcdn.net	27266	10.463019
3	google.com.sg	18751	7.195484
4	messenger.live.com	17345	6.655948
5	www.quora.com	9300	
6	g.doubleclick.net	9779	
7	nyp.edu.sg	8234	
8	clients.google.com	7122	
9	sp.edu.sg	4221	
10	c.youtube.com	3707	

View results

Watching YouTube Videos

1m ago

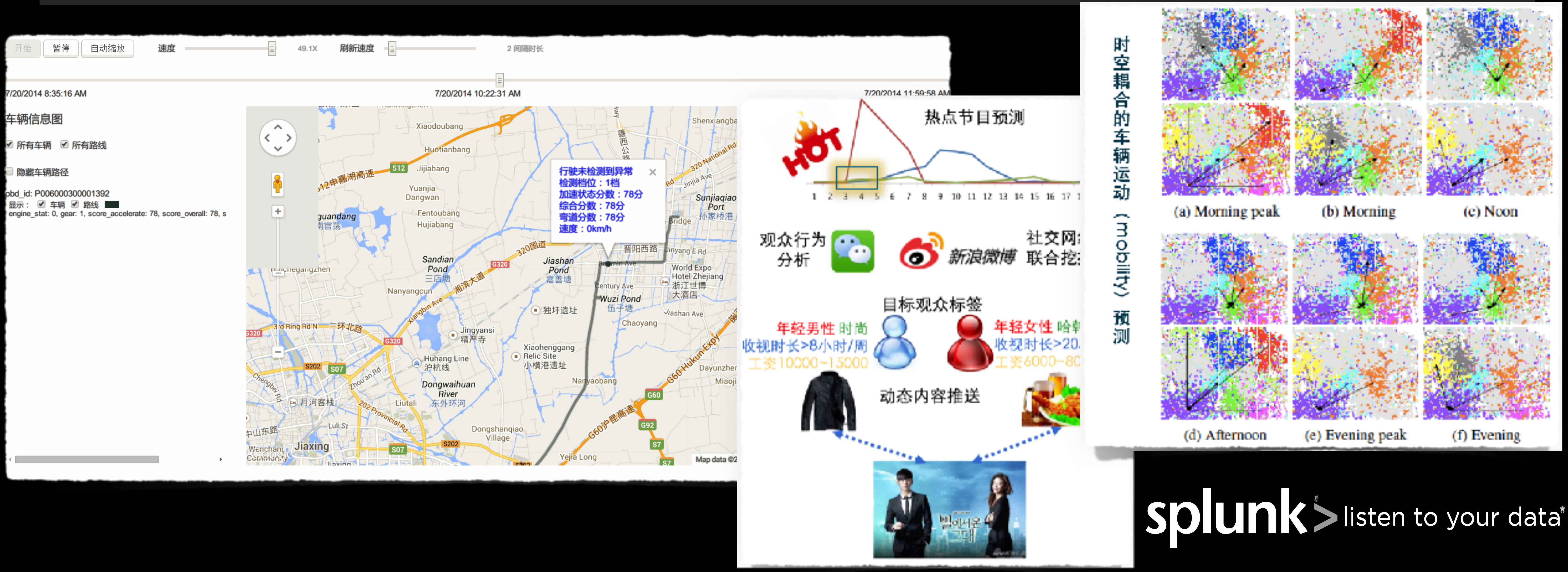
View results

splunk> listen to your data

EDUCATION – SCHOOL INNOVATIVE RESEARCH

大數據與商業創新研究

- 以 Splunk 為基準建立數據決策中心
- 研究跨媒體廣告轉化率(百度等大網站數據導入)對電商影響
- 研究社交網站、內容以及消費媒體關係
- 預測上海市交通阻塞，研究安全駕駛模式及自動駕駛
- 校務管理系統大數據化（不再使用傳統數據庫）
- 定期提供相關資料（大數據/IOT方向）給高校，吸引資優學生入學



obd_id: P006000300001392
显示： ☑ 车辆 ☑ 路线
engine_stat: 0, gear: 1, score_accelerate: 78, score_overall: 78, s

行驶未检测到异常
检测档位：1档
加速状态分数：78分
综合分数：78分
弯道分数：78分
速度：0km/h

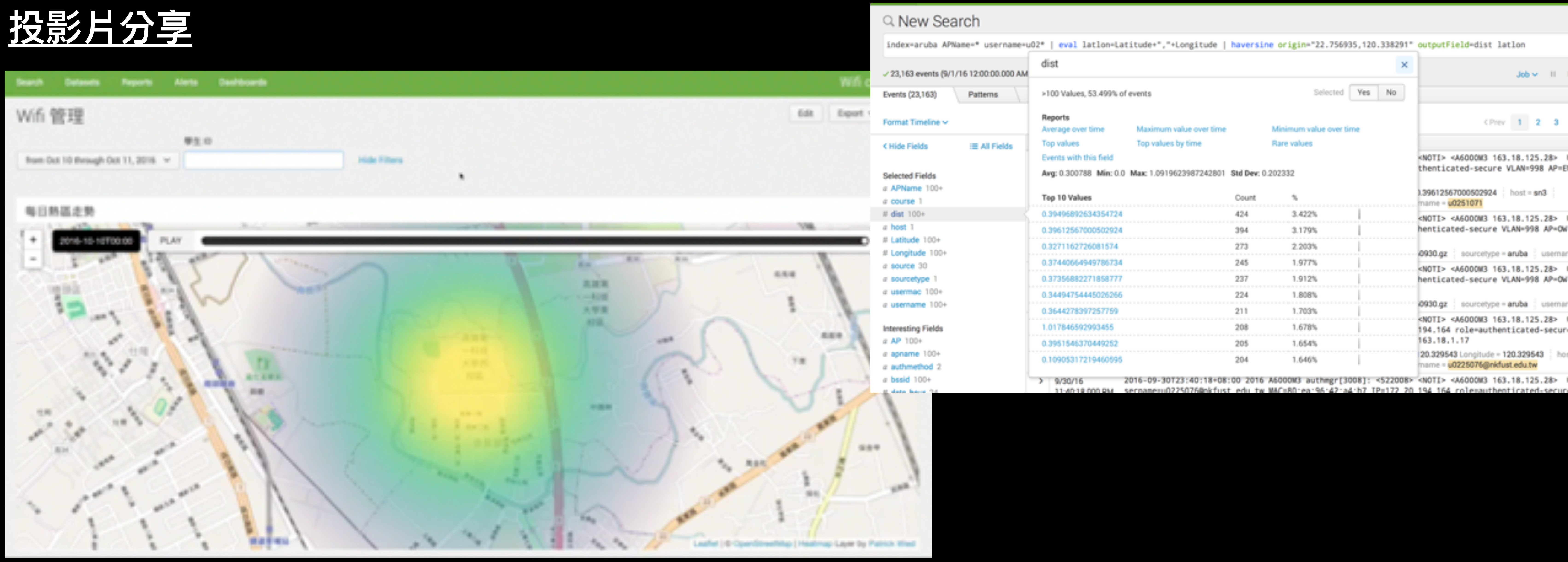
splunk> listen to your data®

EDUCATION – BIG DATA ADOPTION

校務研究、日常運維作業、先進研究等

- WIFI 上網熱點分析
- 透過 WIFI 與學生關聯計算學生出勤課堂比率
- 程式作業追蹤學生作業撰寫狀況
- 餐廳人數追蹤（臨時的行政任務）
- 智慧校園付款系統使用追蹤

投影片分享



```
index=aruba APName=* username=u02* | eval latlon=Latitude+","+Longitude | haversine origin="22.756935,120.338291" outputField=dist latlon
```

✓ 23,163 events (9/1/16 12:00:00.000 AM

Selected Fields
- APName 100+
- course 1
- dist 100+
- host 1
- Latitude 100+
- Longitude 100+
- source 30
- sourcetype 1
- usermac 100+
- username 100+

Interesting Fields
- AP 100+
- apname 100+
- authmethod 2
- bssid 100+

dist

>100 Values, 53.499% of events

Avg: 0.300788 Min: 0.0 Max: 1.0919623987242801 Std Dev: 0.202332

Top 10 Values	Count	%
0.39496892634354724	424	3.422%
0.39612567000502924	394	3.179%
0.3271162726081574	273	2.203%
0.37440664949786734	245	1.977%
0.37356882271858777	237	1.912%
0.34494754445026266	224	1.808%
0.3644278397257759	211	1.703%
1.017846592993455	208	1.678%
0.3951546370449252	205	1.654%
0.10905317219460595	204	1.646%

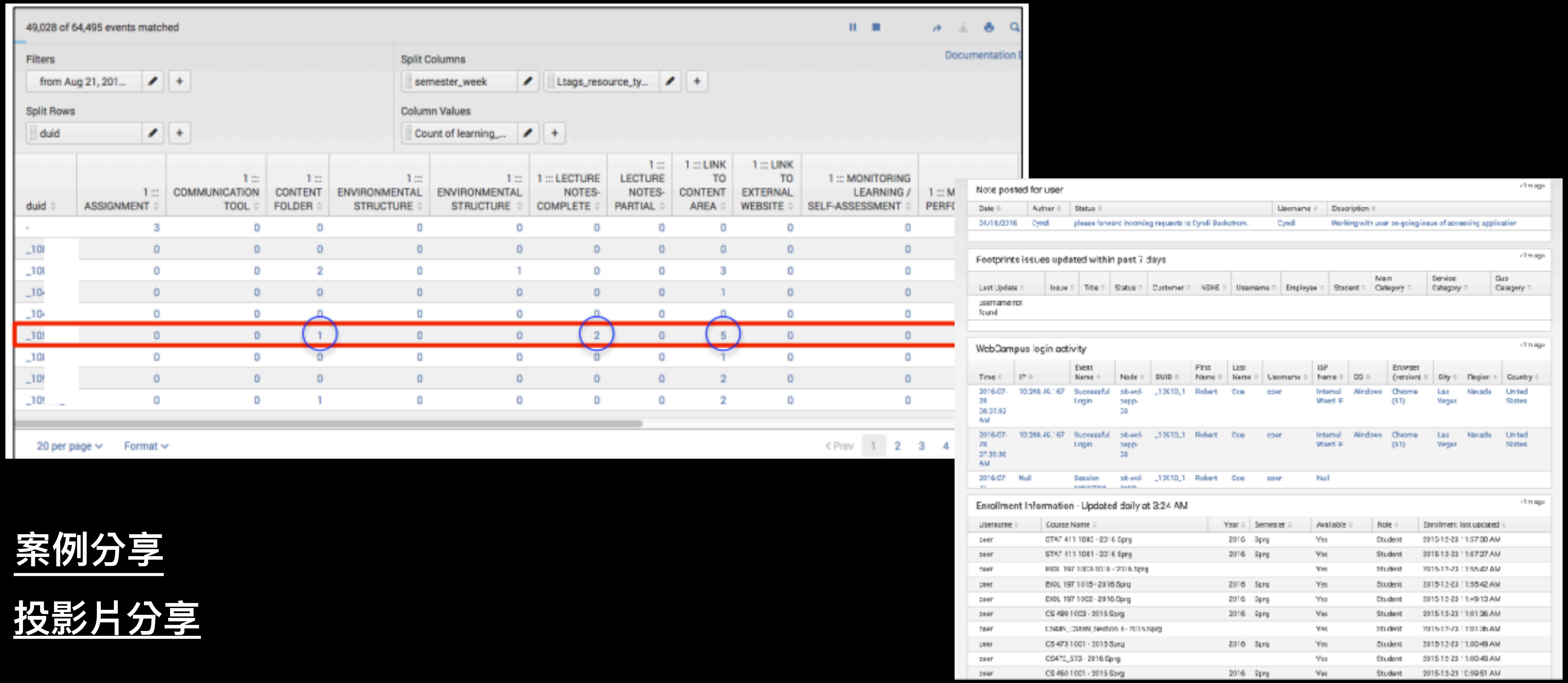
```
<NOTI> <A6000M3 163.18.125.28>
thenticated-secure VLAN=998 AP=E
.39612567000502924   host = sn3
name = u0251071
<NOTI> <A6000M3 163.18.125.28>
henticated-secure VLAN=998 AP=OW
0930.gz   sourcetype = aruba   userna
<NOTI> <A6000M3 163.18.125.28>
henticated-secure VLAN=998 AP=OW
0930.gz   sourcetype = aruba   userna
<NOTI> <A6000M3 163.18.125.28>
194.164 role=authenticated-secur
163.18.1.17
20.329543 Longitude = 120.329543
name = u0225076@nkfust.edu.tw
9/30/16   2016-09-30T23:40:18+08:00 2016 A6000M3 authmgr[3008]: <522008> <NOTI> <A6000M3 163.18.125.28>
```

splunk> listen to your data

EDUCATION – ITOA OPERATIONS

教學研究、日常運維作業等

- 課程學習管理系統效能追蹤
- 學生修課狀況早期預警


49,028 of 64,495 events matched

Filters: from Aug 21, 201...

Split Rows: duid

Split Columns: semester_week, Ltags_resource_ty...

Column Values: Count of learning_...

duid	1 ::: ASSIGNMENT	1 ::: COMMUNICATION TOOL	1 ::: CONTENT FOLDER	1 ::: ENVIRONMENTAL STRUCTURE	1 ::: ENVIRONMENTAL STRUCTURE	1 ::: LECTURE NOTES-COMPLETE	1 ::: LECTURE NOTES-PARTIAL	1 ::: LINK TO CONTENT AREA	1 ::: LINK TO EXTERNAL WEBSITE	1 ::: MONITORING LEARNING / SELF-ASSESSMENT	1 ::: M PERF
-	3	0	0	0	0	0	0	0	0	0	
_10[redacted]	0	0	0	0	0	0	0	0	0	0	
_10[redacted]	0	0	2	0	1	0	0	3	0	0	
_10[redacted]	0	0	0	0	0	0	0	1	0	0	
_10[redacted]	0	0	0	0	0	0	0	0	0	0	
_10[redacted]	0	0	1	0	0	2	0	5	0	0	
_10[redacted]	0	0	0	0	0	0	0	1	0	0	
_10[redacted]	0	0	0	0	0	0	0	2	0	0	
_10[redacted]	0	0	1	0	0	0	0	2	0	0	

Note posted for user <1m ago

Date	Author	Status	Username	Description
04/18/2016	Cyndi	please forward incoming requests to Cyndi Backstrom.	Cyndi	Working with user on-going issue of accessing application

Footprints issues updated within past 7 days <1m ago

Last Update	Issue	Title	Status	Customer	NSHE	Username	Employee	Student	Main Category	Service Category	Sub Category
username not found											

WebCampus login activity <1m ago

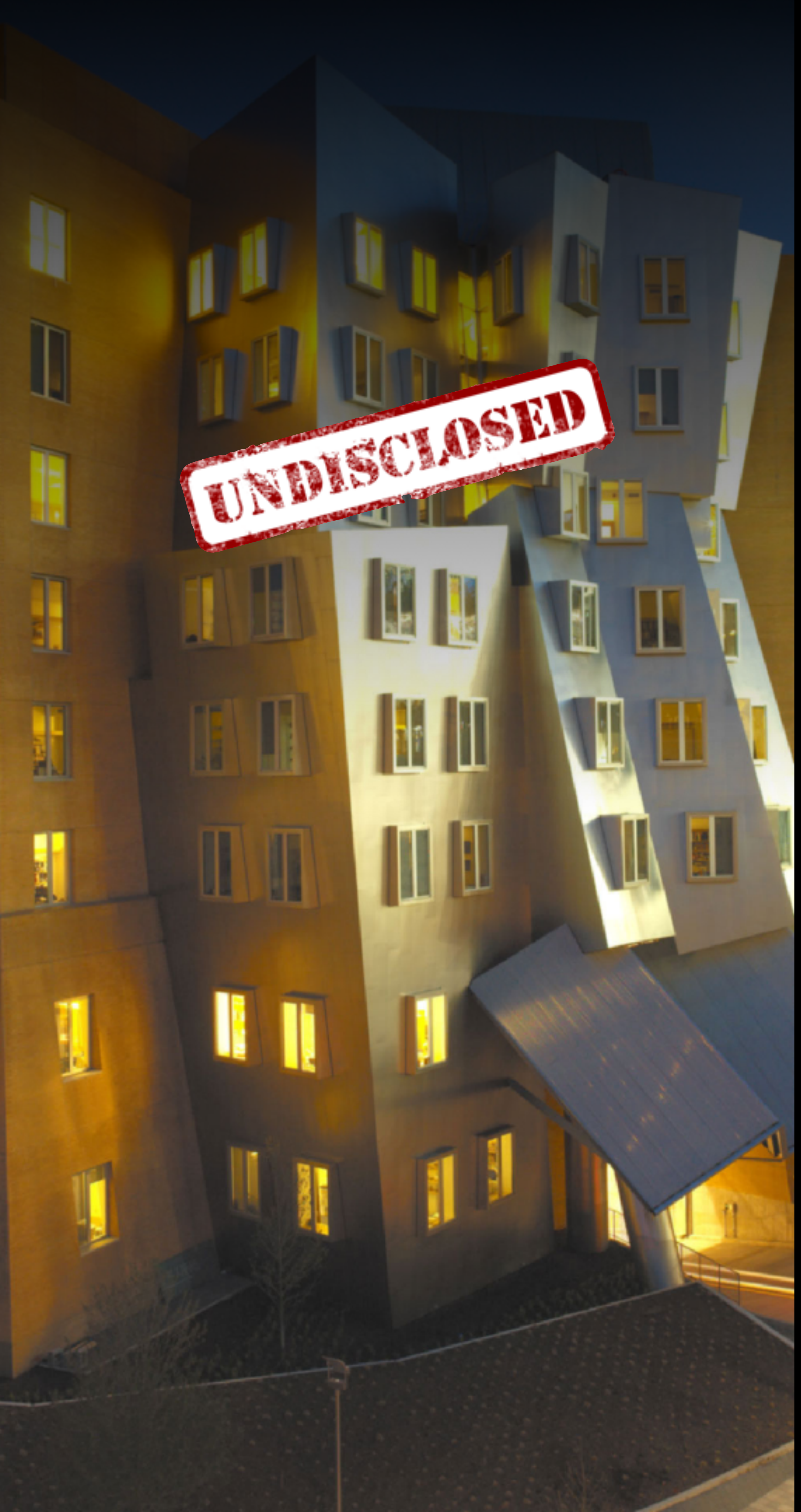
Time	IP	Event Name	Node	BUID	First Name	Last Name	Username	ISP Name	OS	Browser (version)	City	Region	Country
2016-07-28 06:37:02 AM	10.248.40.167	Successful Login	pit-wcl-sapp-03	_13010_1	Robert	Coe	coer	Internal Wlard F	Windows	Chrome (51)	Las Vegas	Nevada	United States
2016-07-28 07:35:36 AM	10.248.40.167	Successful Login	pit-wcl-sapp-03	_13010_1	Robert	Coe	coer	Internal Wlard F	Windows	Chrome (51)	Las Vegas	Nevada	United States
2016-07-	Null	Session	pit-wcl-	_13010_1	Robert	Coe	coer	Null					

Enrollment Information - Updated daily at 3:24 AM <1m ago

Username	Course Name	Year	Semester	Available	Role	Enrollment last updated
coer	STAT 411 1080 - 2016 Sprg	2016	Sprg	Yes	Student	2015-12-23 11:57:30 AM
coer	STAT 411 1081 - 2016 Sprg	2016	Sprg	Yes	Student	2015-12-23 11:57:27 AM
coer	BIOL 197 1003-1018 - 2016 Sprg			Yes	Student	2015-12-23 11:55:47 AM
coer	BIOL 197 1015 - 2016 Sprg	2016	Sprg	Yes	Student	2015-12-23 11:55:42 AM
coer	BIOL 197 1002 - 2016 Sprg	2016	Sprg	Yes	Student	2015-12-23 11:49:13 AM
coer	CS 489 1003 - 2015 Sprg	2016	Sprg	Yes	Student	2015-12-23 11:01:26 AM
coer	CS489_CS689_Section 1 - 2015 Sprg			Yes	Student	2015-12-23 11:01:26 AM
coer	CS 473 1001 - 2015 Sprg	2016	Sprg	Yes	Student	2015-12-23 11:00:49 AM
coer	CS472_573 - 2016 Sprg			Yes	Student	2015-12-23 11:00:49 AM
coer	CS 460 1001 - 2015 Sprg	2016	Sprg	Yes	Student	2015-12-23 10:59:51 AM

案例分享

投影片分享

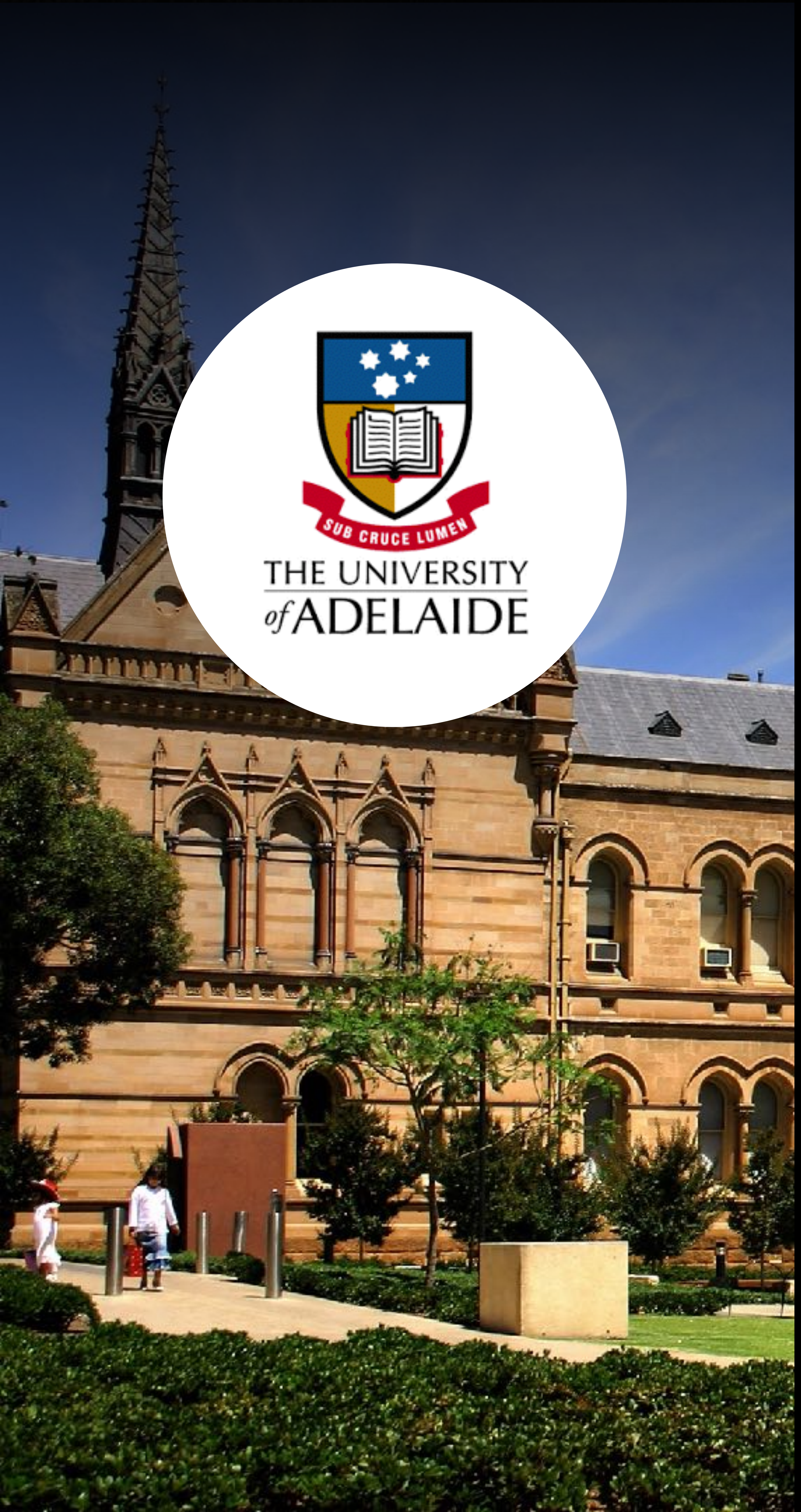


EDUCATION – BUSINESS ANALYTICS

校園資源分析應用案例

- ▶ 期刊訂閱追蹤
- ▶ 校園筆電使用/學生上課追蹤
- ▶ 對外開放課程學生追蹤
- ▶ 預測對外網路流量成長
- ▶ 學生就業/入學前追蹤選課成績 (Outliers 分析)

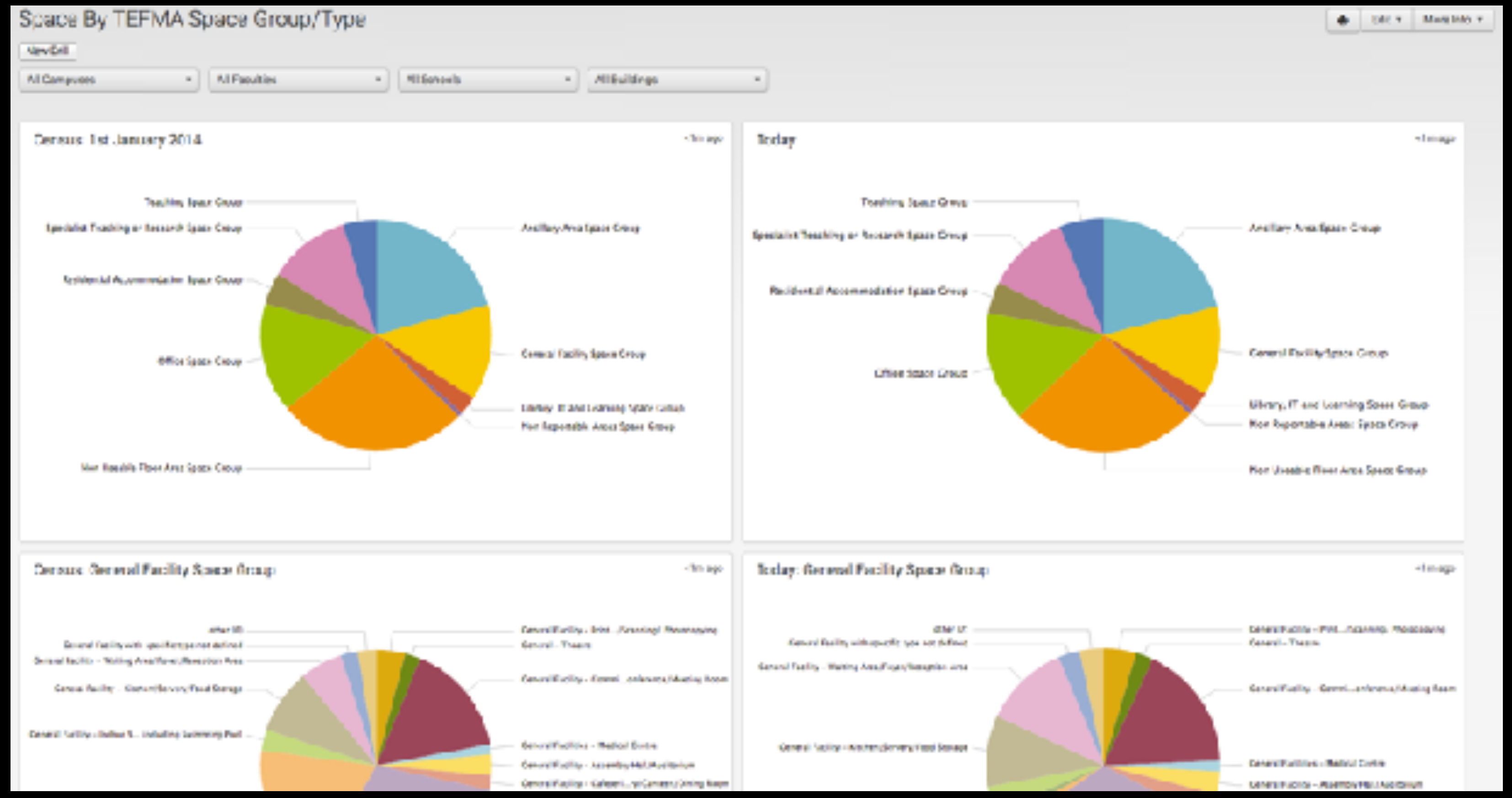
Data sources: 入學成績, 學生資料庫, 期刊 proxy, vpn, wifi, 校友紀錄

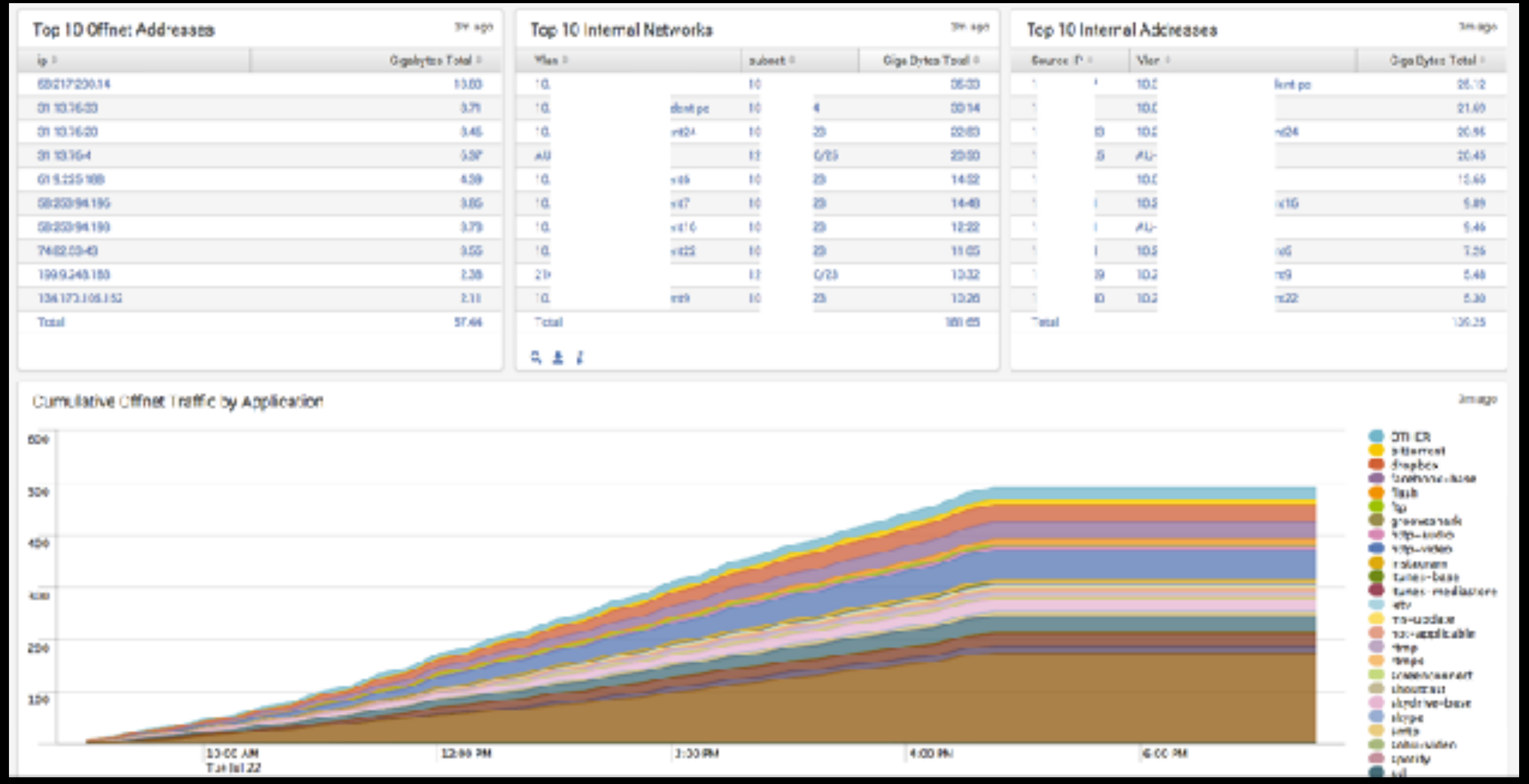


EDUCATION – SECURITY

營運透明度提升系統效能及簡化資源規劃

- ▶ 資安入侵調查/回應 (SOC 中心)
- ▶ 日常業務簡化/報告自動化
- ▶ 列印記錄、學生/校外上網記錄分析
- ▶ 實體空間(教室/實驗室/校園設施)使用報告/排程


Space By TEFMA Space Group/Type
All Campuses
All Faculties
All Schools
All Buildings
Census 1st January 2014
Today
Teaching Space Group
Specialist Teaching or Research Space Group
Residential Accommodation Space Group
Office Space Group
Ancillary Area Space Group
General Facility Space Group
Library, IT and Learning Space Group
Non Reportable Areas Space Group
Non Useable Floor Area Space Group
Census: General Facility Space Group
Today: General Facility Space Group



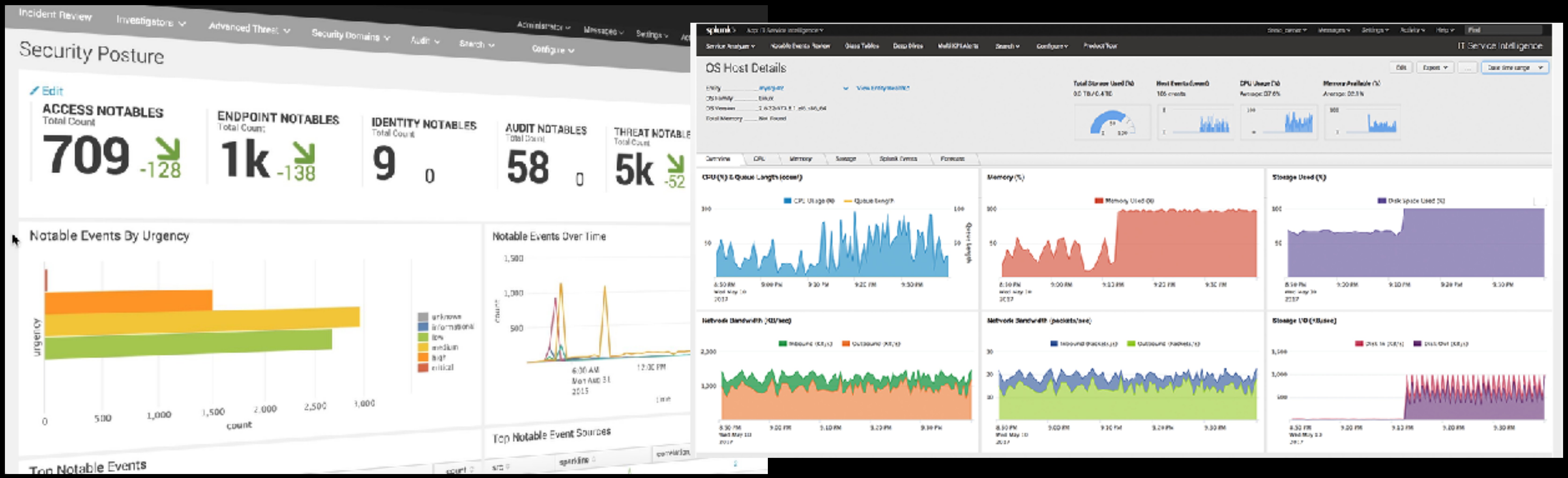
> “ Previously it could take hours to extract and analyze logs to identify security issues–now it can be measured in minutes. Splunk has given us the highest degree of certainty in meeting our immediate and future security needs.”
>
> – ***Information Security Specialist, University of Adelaide***

splunk> listen to your data®

EDUCATION – SECURITY, IT OPERATIONS

校園資料完整性追蹤及帶來快速人力投資回報

- 每月節省超過 $25,000+ 美金頻寬支出
- 增加校園安全視圖，更主動的監控以及快速的威脅處理
- 減少用戶打電話到服務台的需要增加用戶良好體驗

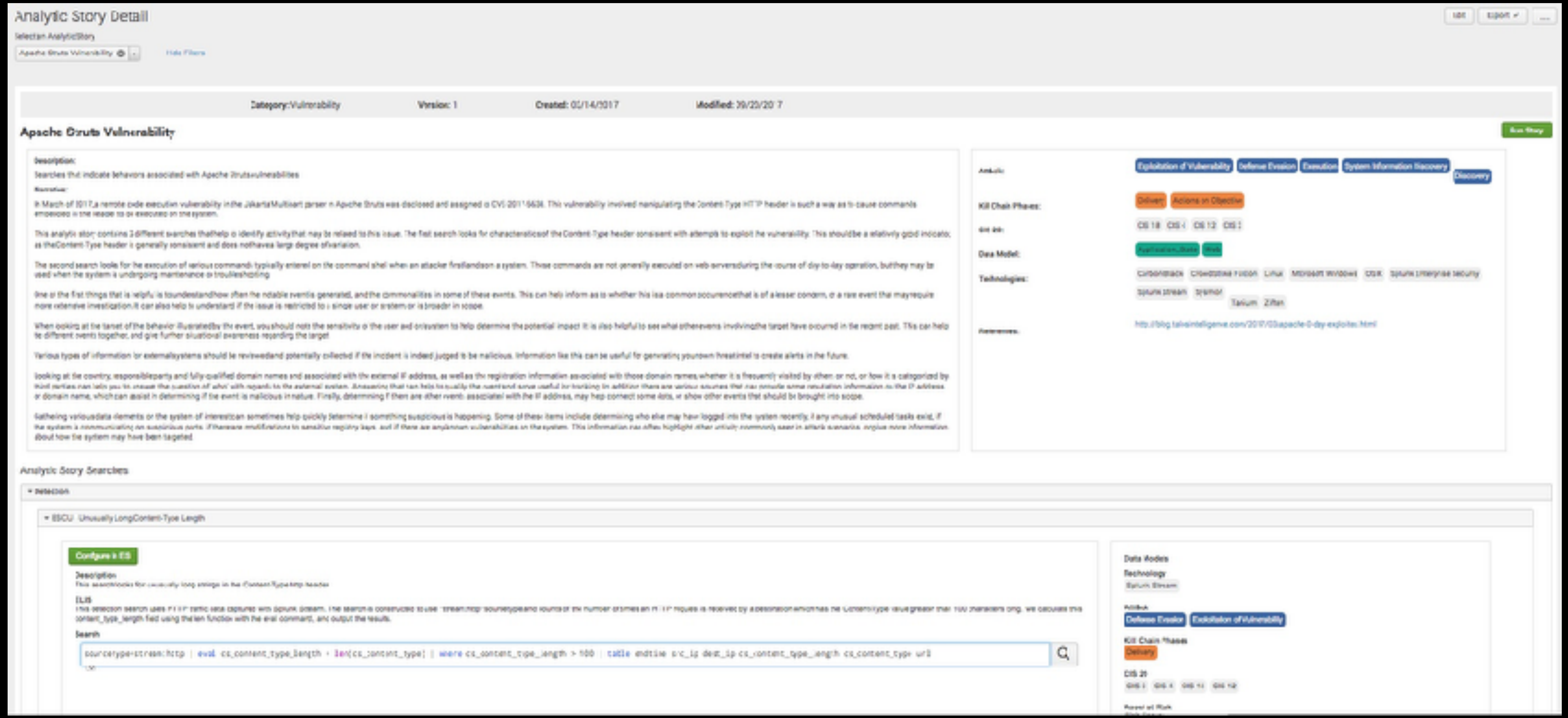


> “ Splunk software can index any data and help you to create meaningful reports for any situation. I have learned to throw as much data as possible at Splunk. The more you use it, the more value you get from it.”
>
> - Systems Architect, American University of Sharjah

EDUCATION – SECURITY

提供更好的服務

- 自動化的SOC規則更新大幅節省人力進行安全追蹤
- 提升服務流程品質達到更好的雇員/學生體驗
- 透過機器學習套件找出更多安全問題強化系統安全


Analytic Story Detail
Category: Vulnerability
Version: 1
Created: 03/14/2017
Apache Struts Vulnerability
Description:
Narrative:
ATT&CK:
Kill Chain Phases:
Data Model:
Technologies:
References:
Analytic Story Searches
Detection
ESCU - Unusually Long Content-Type Length
Configure in ES
Description
Search
sourcetype=stream:http | eval cs_content_type_length = len(cs_content_type) | where cs_content_type_length > 100 | table endtime src_ip dest_ip cs_content_type_length cs_content_type url

> “ Splunk Enterprise has helped us tackle phishing attacks so we are no longer blacklisted by email providers. Not only can we now deliver an uninterrupted service to our users, but we’ve saved weeks of manpower.”
>
> - System Administrator, Maastricht University

針對學校研究 Splunk 能提供的協助

Programs

非營利組織(包含學校), 開發者, 研究者等

在課堂教學使用或是研究室研究 Splunk:

https://www.splunk.com/en_us/about-us/splunk-pledge/academic-license-application.html

Splunk provides a **one-year, 10GB license for Splunk software** and access to eLearning to qualifying not-for-profit universities **at no cost**. To qualify, your school must be an accredited not-for-profit institution of higher education and use the license and eLearning for teaching purposes only.

Splunk will provide free software, standard support, and **complimentary access to Splunk eLearning for all Splunk Academic Partners, and complimentary access to Splunk eLearning for all qualifying students.**

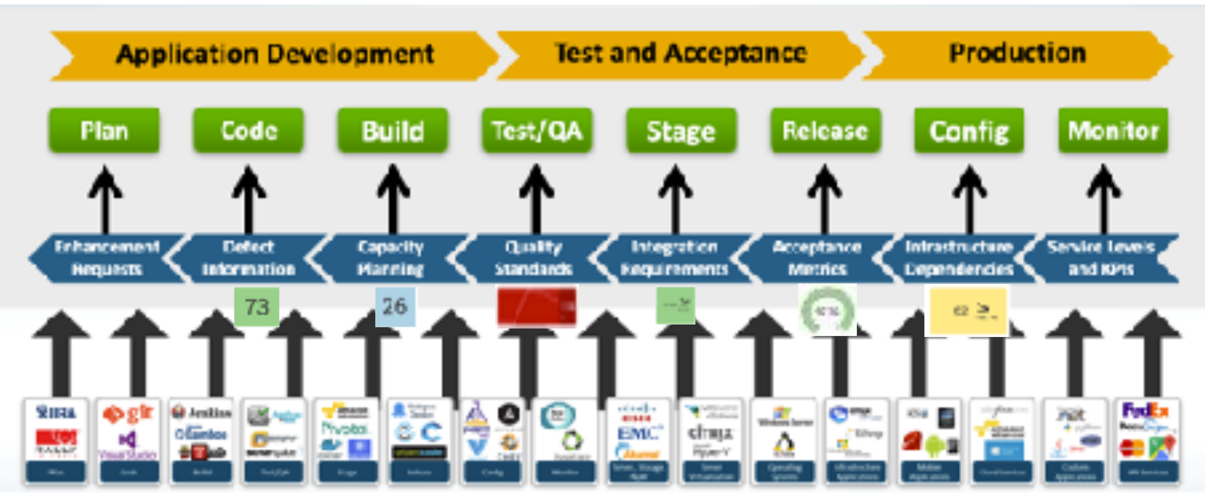
研究 Splunk 相關整合、進階開發者:

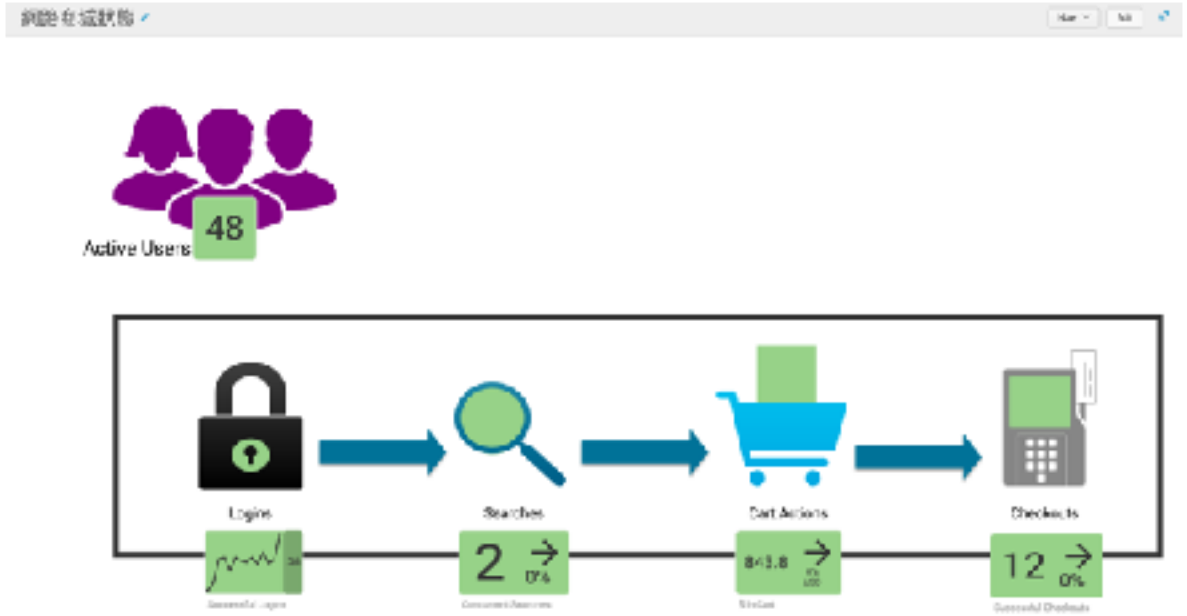
http://dev.splunk.com/page/developer_license_sign_up/

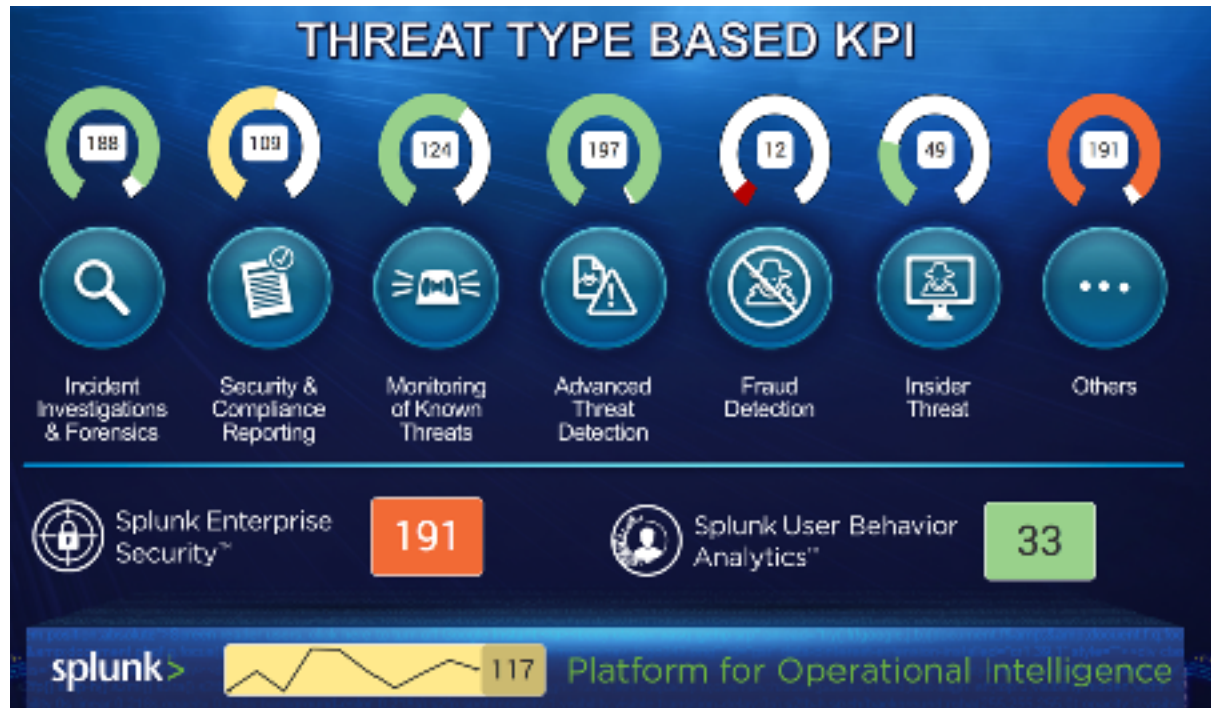
Developer Trial License

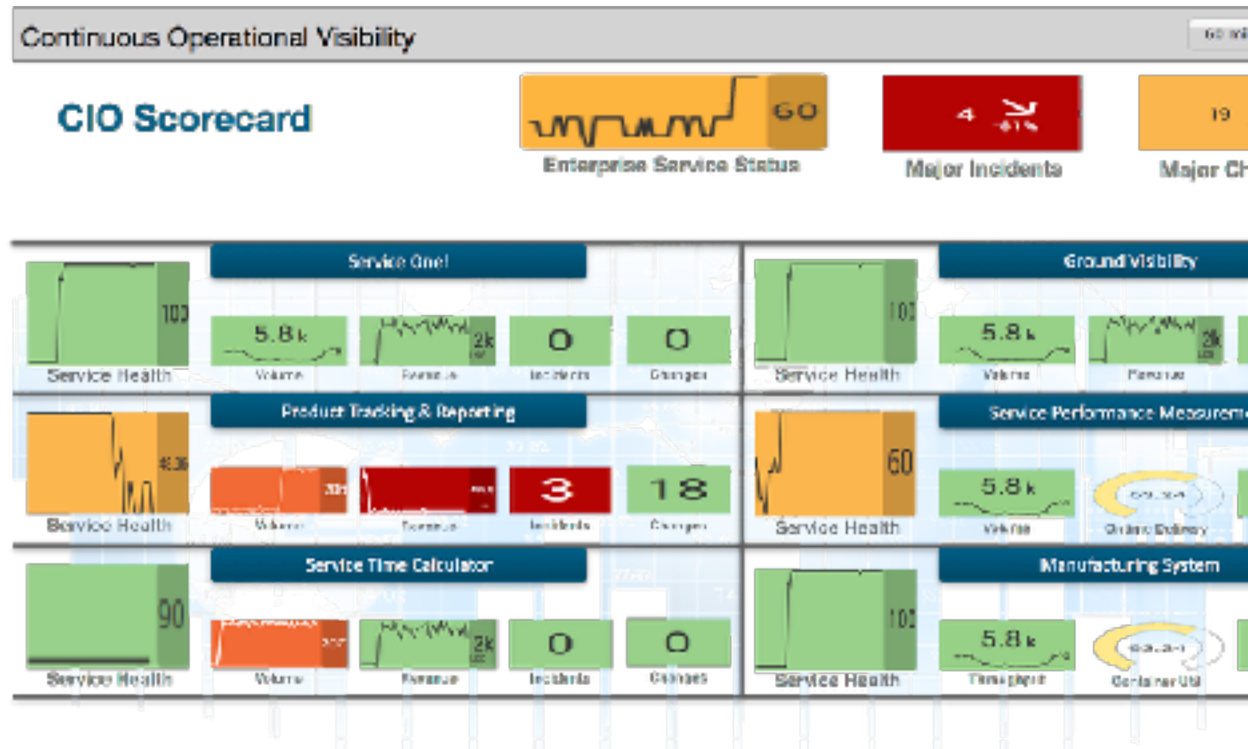
- 10 GB of daily indexing
- Full enterprise features
- Free trial for 6 months

將 IT/資安/服務 管理變成整體營運戰略中心






THREAT TYPE BASED KPI
188
109
124
197
12
49
191
Incident Investigations & Forensics
Security & Compliance Reporting
Monitoring of Known Threats
Advanced Threat Detection
Fraud Detection
Insider Threat
Others
Splunk Enterprise Security
191
Splunk User Behavior Analytics
33
splunk>
117
Platform for Operational Intelligence



- SoC/NoC/IToC —> Business Operation Centre(BoC)
- 實際監控分析重要業務服務以及客戶體驗

splunk>