巨量安全資料的專業分析家

—IMPERVA幫助您從巨量的Web與資料庫的安全事件中，分析出真正需要關心的事件

IMPERVA台灣資深技術顧問 范鴻志 Holmes Fan

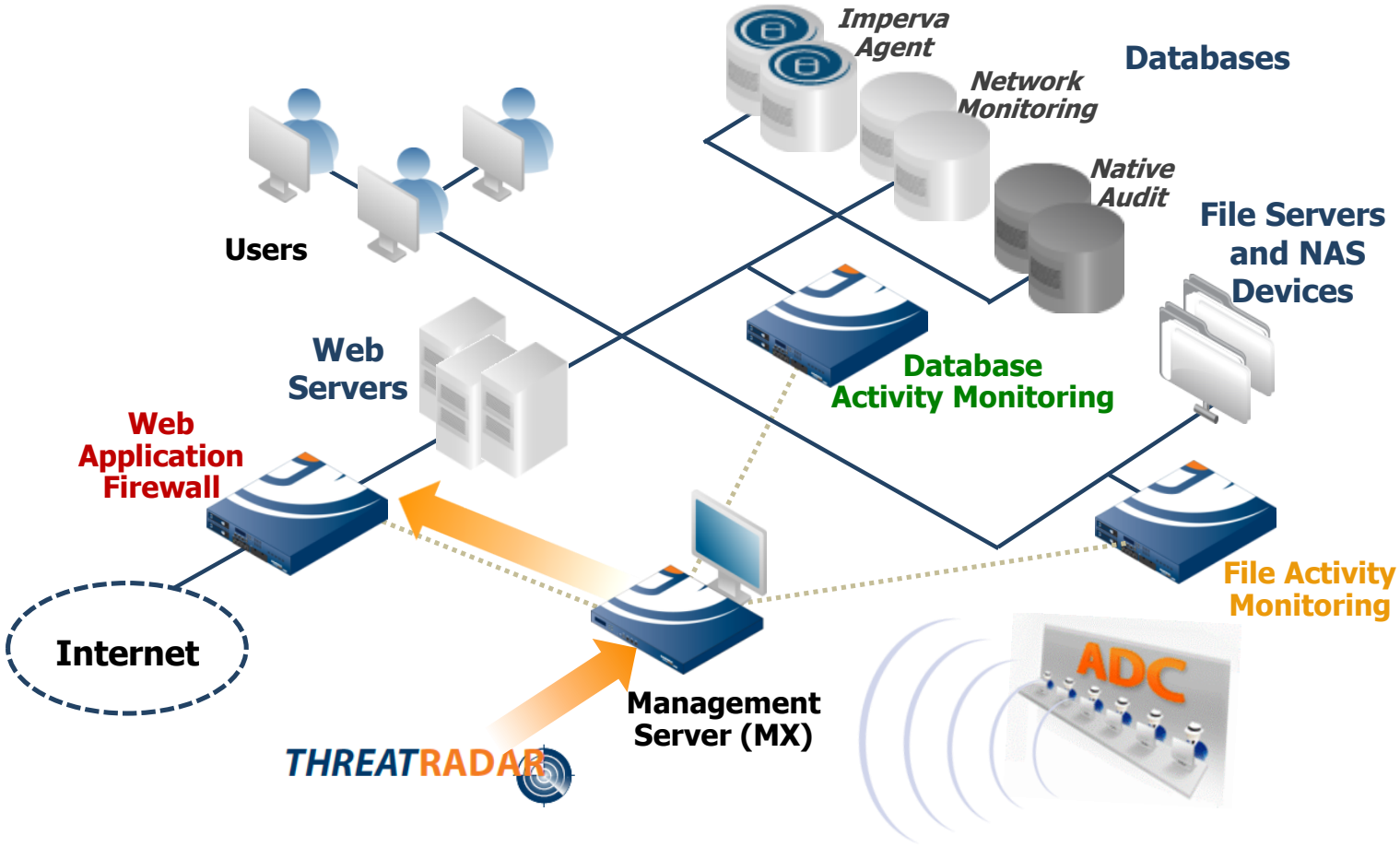
9/11/2018

IMPERVA®

IMPERVA公司簡介

- IMPERVA於2002年由Shlomo Kramer創立，他是網路資安設備領導廠商Check point的創始股東之一，並於2008年榮獲SC雜誌評選為年度CEO，公司股票於2011.11於美國證交所(IMPV)上市，公司人數超過1000人，R&D與技術人員佔6成。
- IMPERVA致力於保護企業內部之重要資料，包括儲存於資料庫伺服器(Database Server)或是檔案伺服器(File Server)中之資料，不管是內部對資料庫及檔案伺服器的不友善或未授權之存取，或是來自外部對web server及資料庫的威脅，IMPERVA皆可做到有效的防護，以降低企業敏感資料外洩之機率。
- IMPERVA目前於全球超過100個國家有使用客戶，已有超過3300家客戶使用，各個產業皆有採用IMPERVA解決方案之客戶，如政府、電信、金融、電子商務、製造業等各個領域。於台灣也已有超過230家客戶使用，且使用客戶正持續快速增加中。

IMPERVA幫助企業保護重要資料，是企業資料保護的專家



人與訊息(Message or information)的關係

製造者(Creator)

接收者(Receiver)

傳遞者(Forwarder)

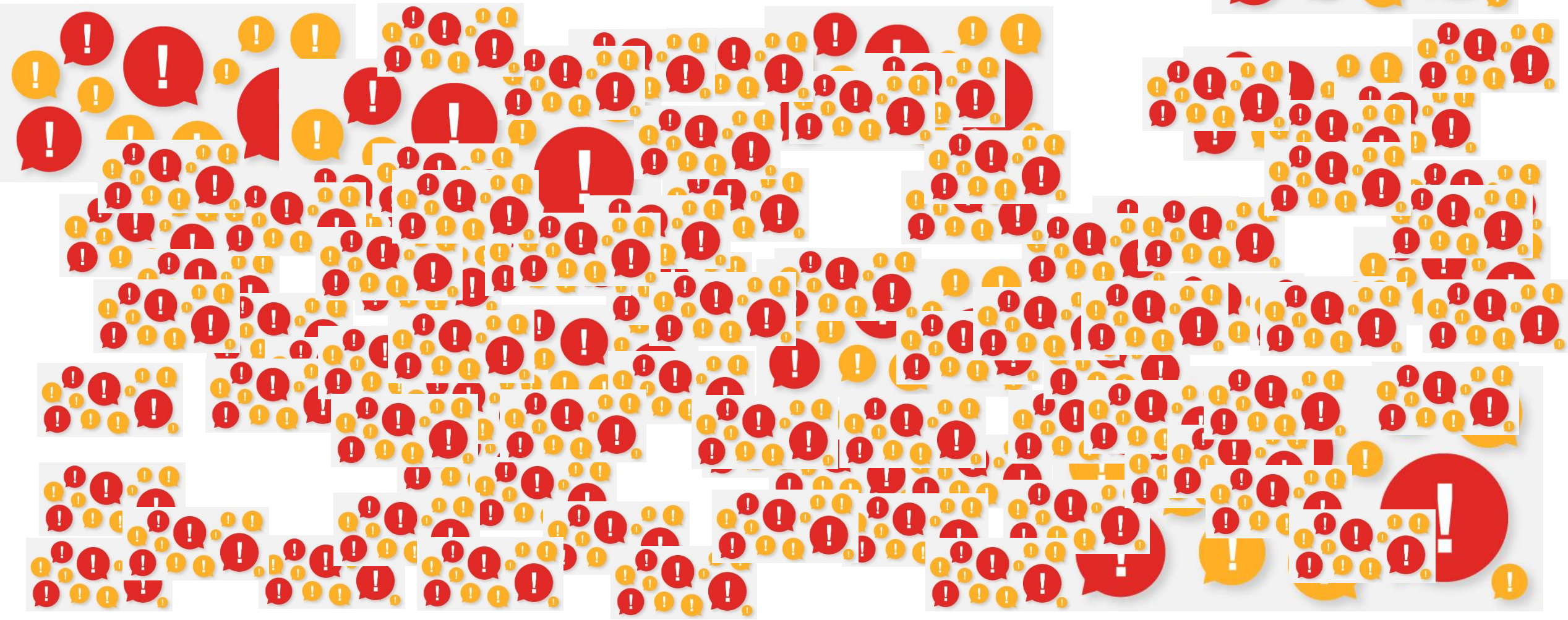
User與資安訊息的關係則是

User大部分是資安訊息的被動接收者(Receiver)，少部分是傳遞者(Forwarder)

資安新知
資安新聞
&
為數眾多的資安Log

數大便是美？

Security alerts volume is increasing



我們不要讓這些為數眾多
的資安Log變成無用資訊

但不知如何消化
不知那些才是真正重要的

Log Server or SIEM?

Log Server-眾多異質Log的收集與正規化的獨立儲存設備，有需求時就可查詢。-完全被動

SIEM-能力較強的Log Server，具有關聯分析的能力，可主動告警(但必須先設定告警規則)。-大部分被動，少部分主動(且要依據管理者所設定的規則)

人力成本與機會成本

我們應該主動發現，而非被動回應

而且不增加人力成本甚至可降低

「去蕪存菁」的人工智慧

- 無以計數的資料庫稽核紀錄(Database Auditing Logs)或是網站攻擊事件(WAF Security Events)，讓您無法消化
- IMPERVA藉由機器學習與人工智慧幫助您從巨量的事件資訊中找出極少量具高價值的事件，對資訊安全有極大的幫助

人工智慧

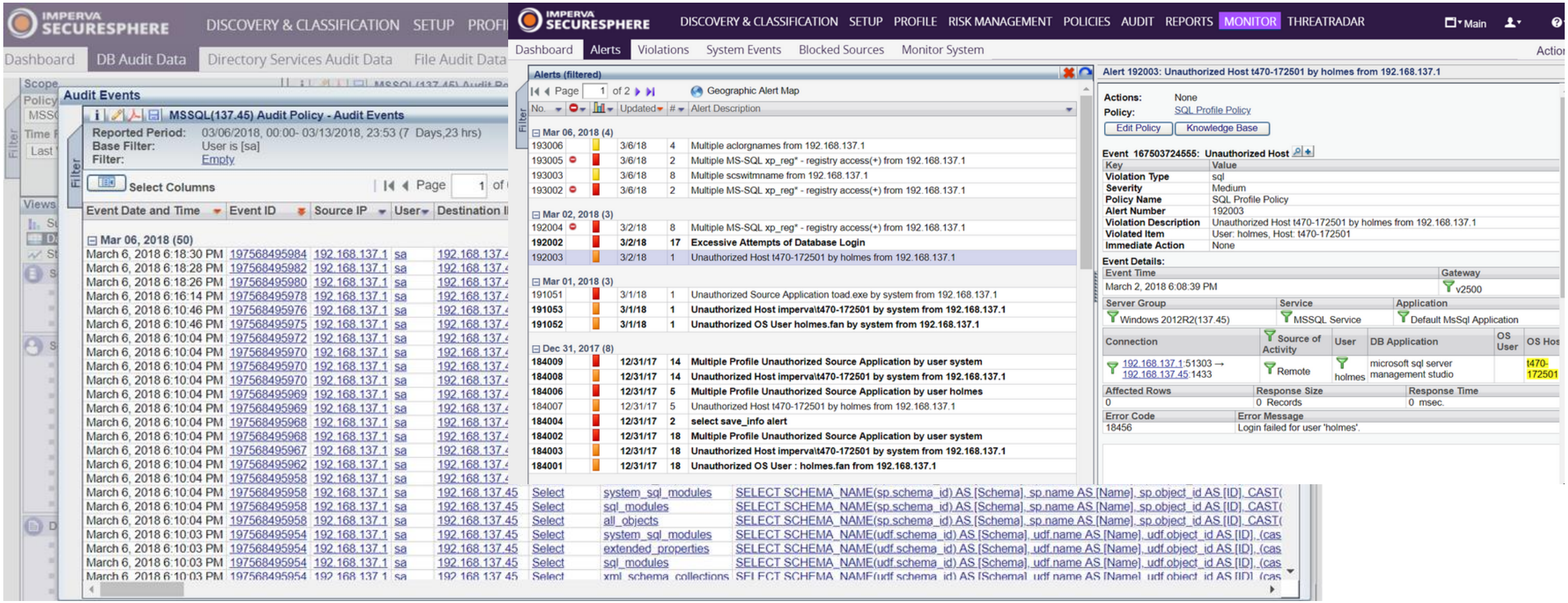
機器學習

IMPERVA®

IMPERVA® COUNTERBREACH

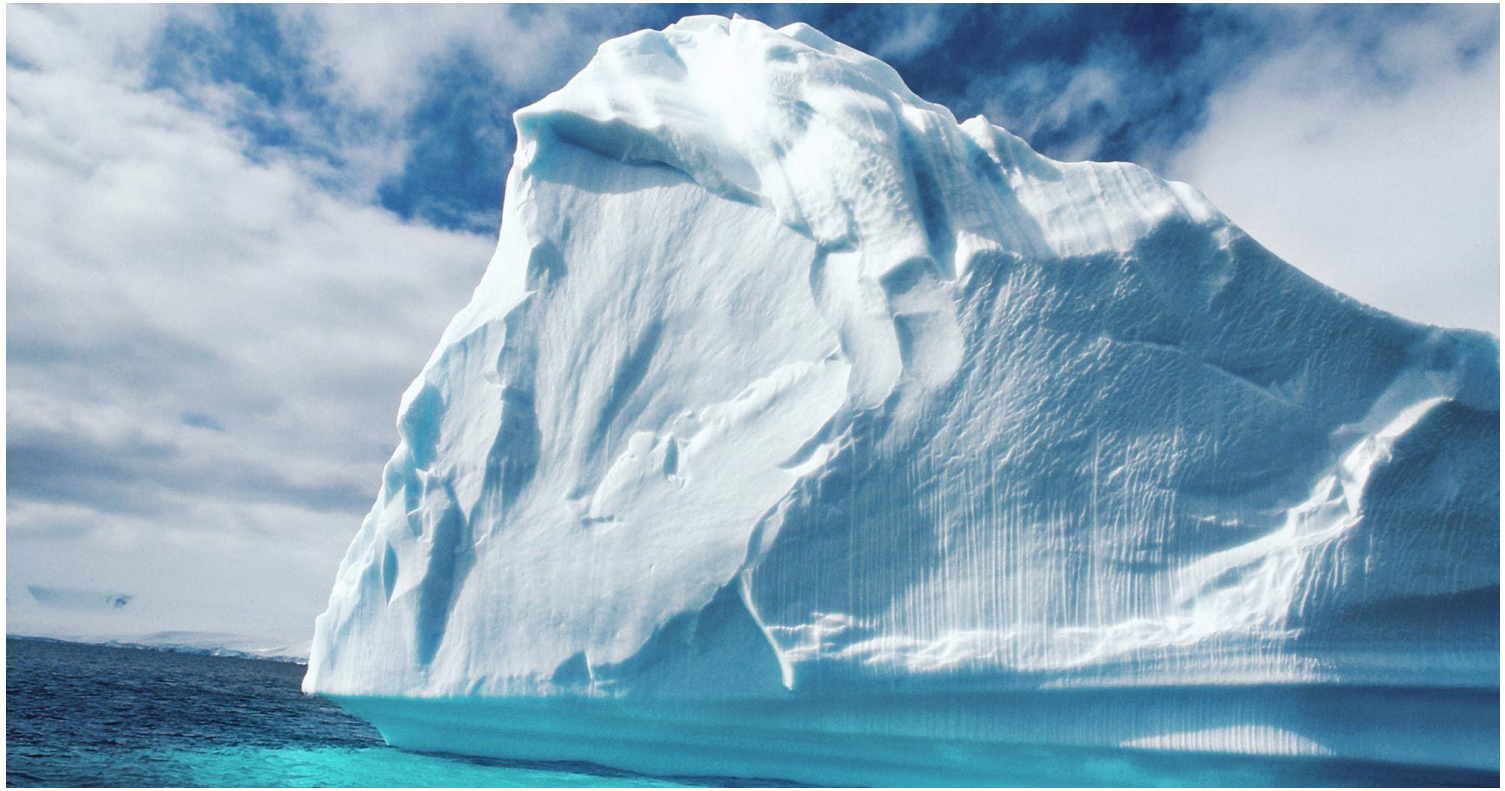
IMPERVA®

IMPERVA DAM可以幫您做到必須要做的資料庫稽核及安全



IMPERVA

但稽核事件量如冰山巨大



要想從中找到反常事件，有如大海撈針

IMPERVA CounterBreach 機器學習與人工智慧可以幫助您

持續動態(Dynamic)濾除絕大多數規律化正常行為

取得更多的機會，主動發現極少數的反常行為

降低敏感資料被不當使用或被竊取的風險

事件分析五個基本元素

- 人
- 事
- 時
- 地
- 物

使用者使用被授權的帳號於適當的時間在正確的地方利用合法的方式做對的事

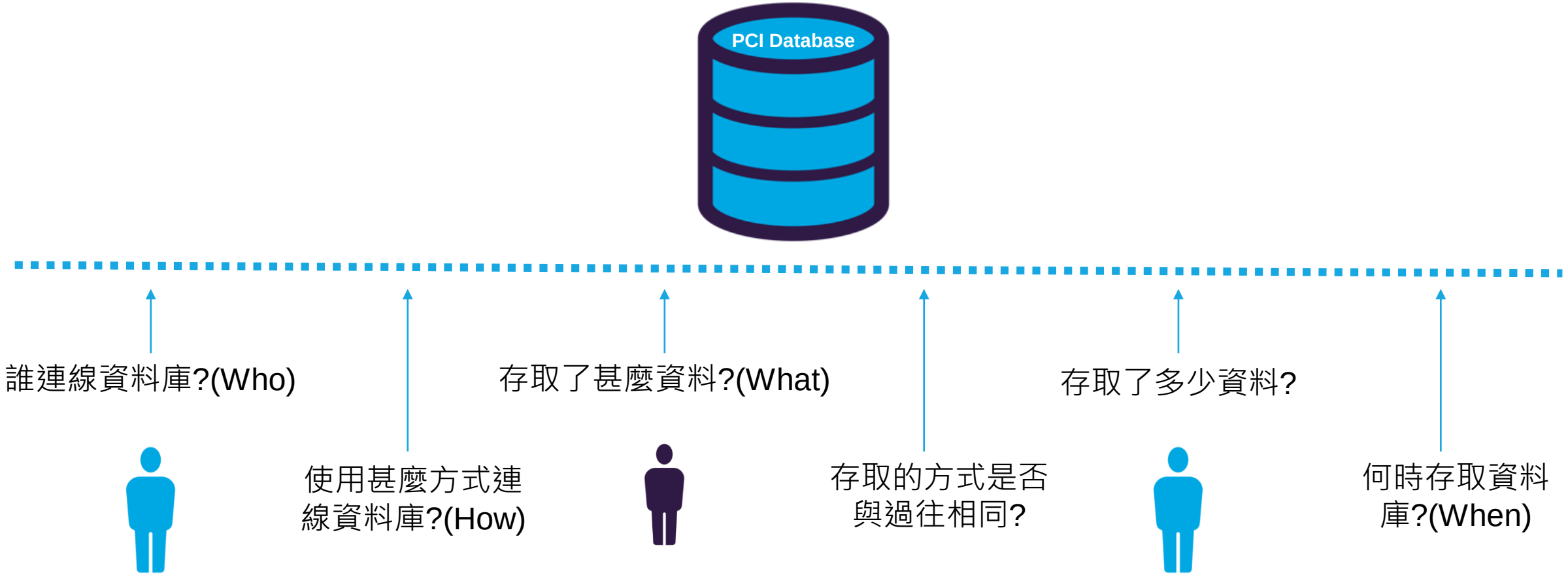
CounterBreach 偵測與輔助控制不當資料存取行為

監控與資料收集
(DAM,DBF)
MONITOR

學習與偵測
(CounterBreach)
LEARN AND DETECT

安全管控(告警或阻擋)
(DAM,DBF)
BLOCK /
QUARANTINE

Behavior: 建立使用者存取資料庫的判斷基準線(Baseline)

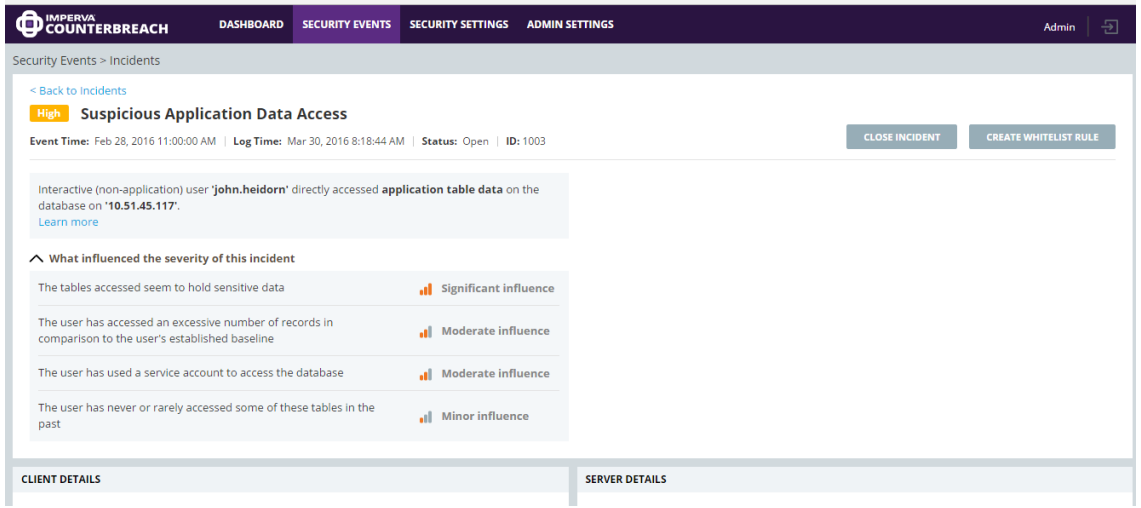


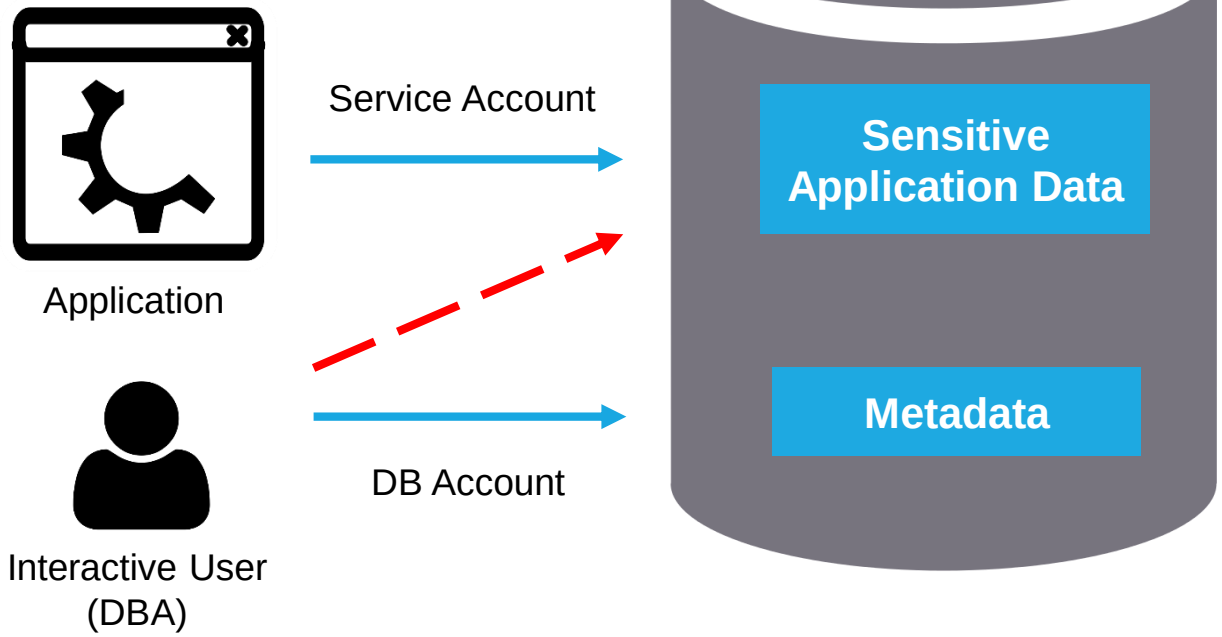
IMPERVA®

情境一 – Suspicious Application Data Access
(應用程式資料被其他user直接存取)

Detect

- Identify compromised, careless and malicious users
  - Application Data Access





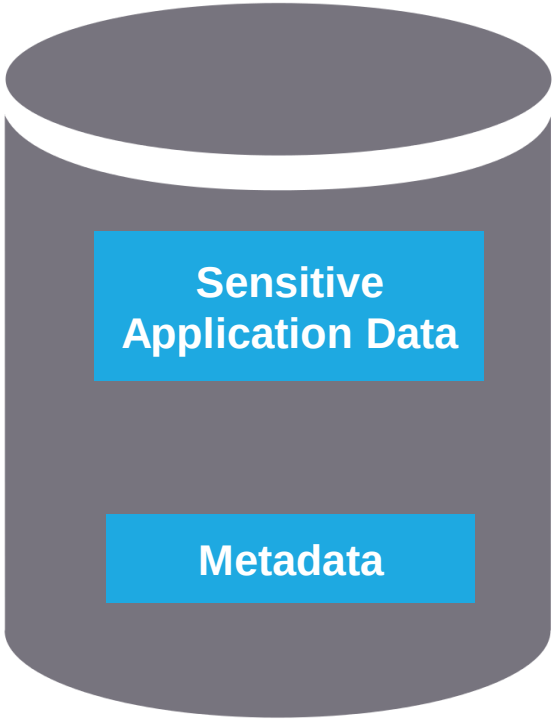
情境二– Service Account Abuse
（應用程式帳號被濫用）

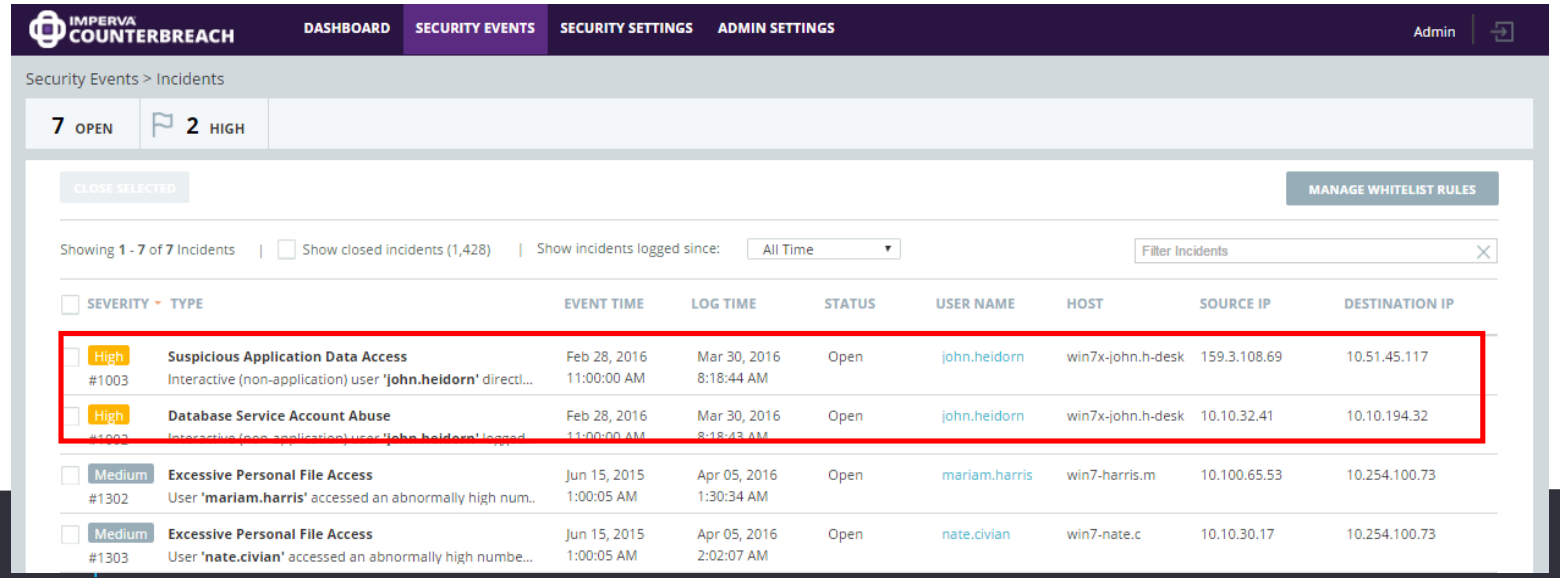
Detect

- Identify compromised, careless and malicious users
  - Application Table Access
  - Service Account Abuse

Interactive User

Service Account



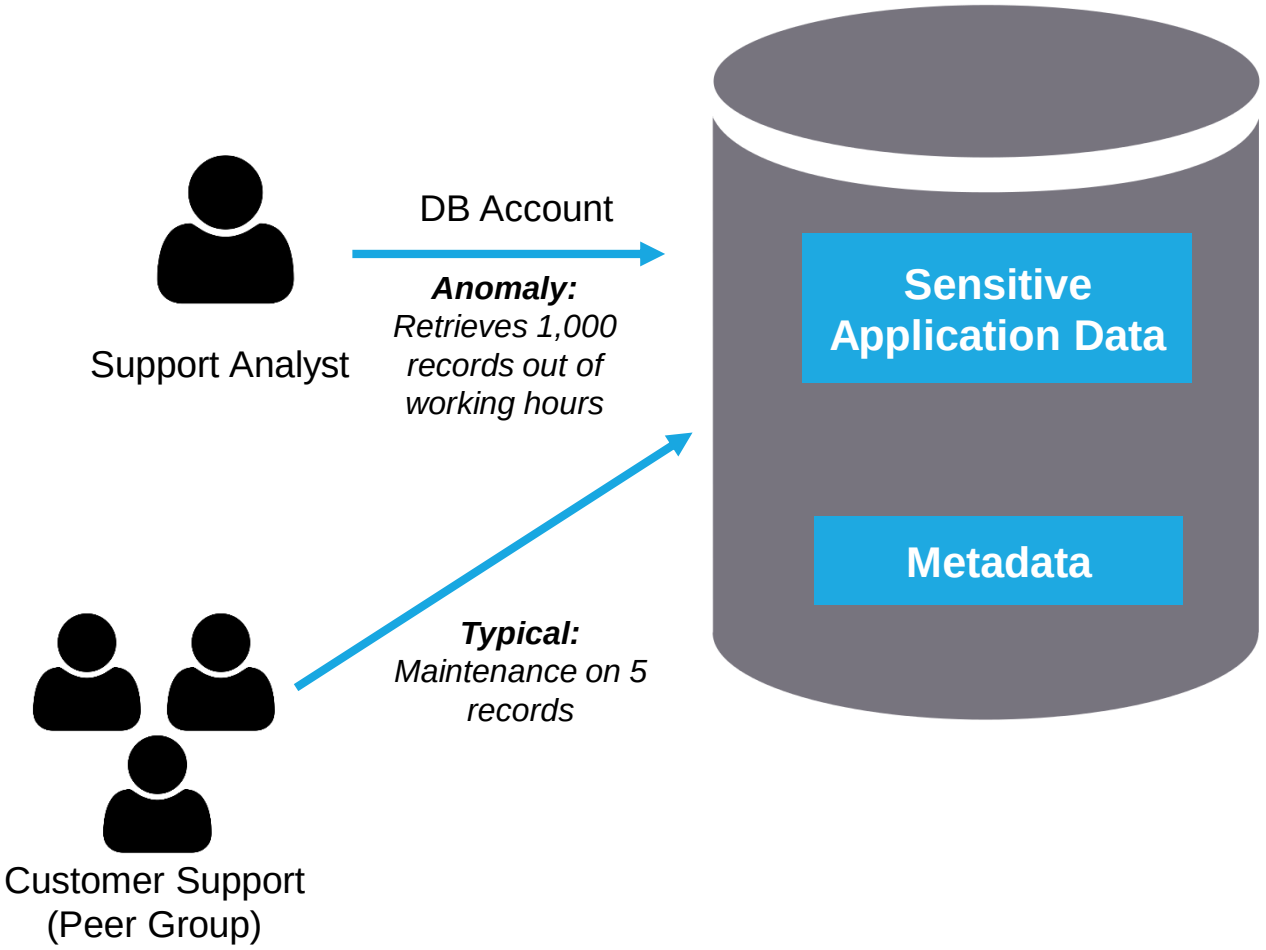


IMPERVA®

情境三– Excessive Data Access
（存取過量資料）

Detect

- Identify compromised, careless and malicious users
  - Application Table Access
  - Service Account Abuse
  - Unusual Data Retrieval



IMPERVA®

The CounterBreach Difference
Financial Services

Before
- 2% of databases monitored
- 0.25 FTE
- 1,000 alerts per day
- 1% of alerts investigated
- 0 significant incidents discovered

After
- 50% of databases monitored
- 0.25 FTE
- 15-30 alerts per day
- 100% of alerts investigated
- 2 significant incidents discovered

Results
- 25x more databases monitored
- Equivalent FTE
- 1000x reduction in rate of alerts
- 100x increase in alerts investigated

CounterBreach improved effectiveness of data security without increased labor costs

IMPERVA®

對於資料庫安全，主動優於被動

以最精簡的人力及最少的時間，配合聰明智能化的資料庫行為分析系統(IMPERVA CounterBreach)，達到最有效之資料庫使用行為風險分析、統計與管控。

Imperva Attack Analytics

IMPERVA®

Situation At-A-Glance

55%

每日安全事件數量
超過10,000筆

57%

調整政策
以降低事件量

54%

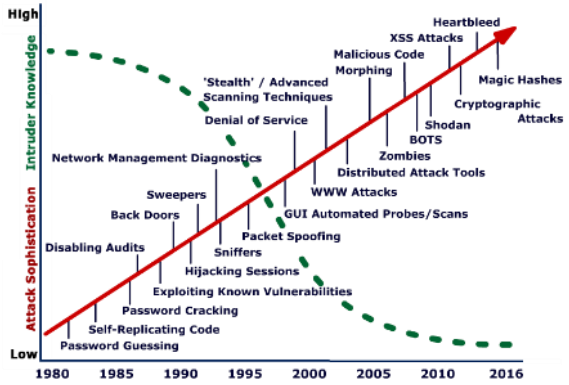
因為龐大的安全事件
量而不知所措

Imperva Survey at RSA Security Conference 2018

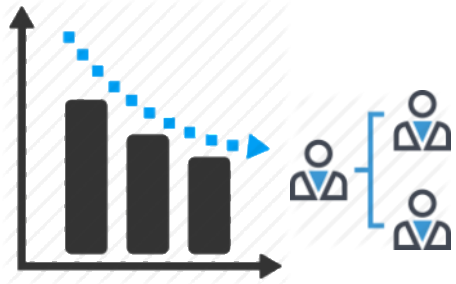
IMPERVA®

WHY?

安全事件數量
持續大量增加



攻擊手法不斷翻新
及
攻擊涵蓋面持續擴增



安全事件分析專
業人員的缺乏

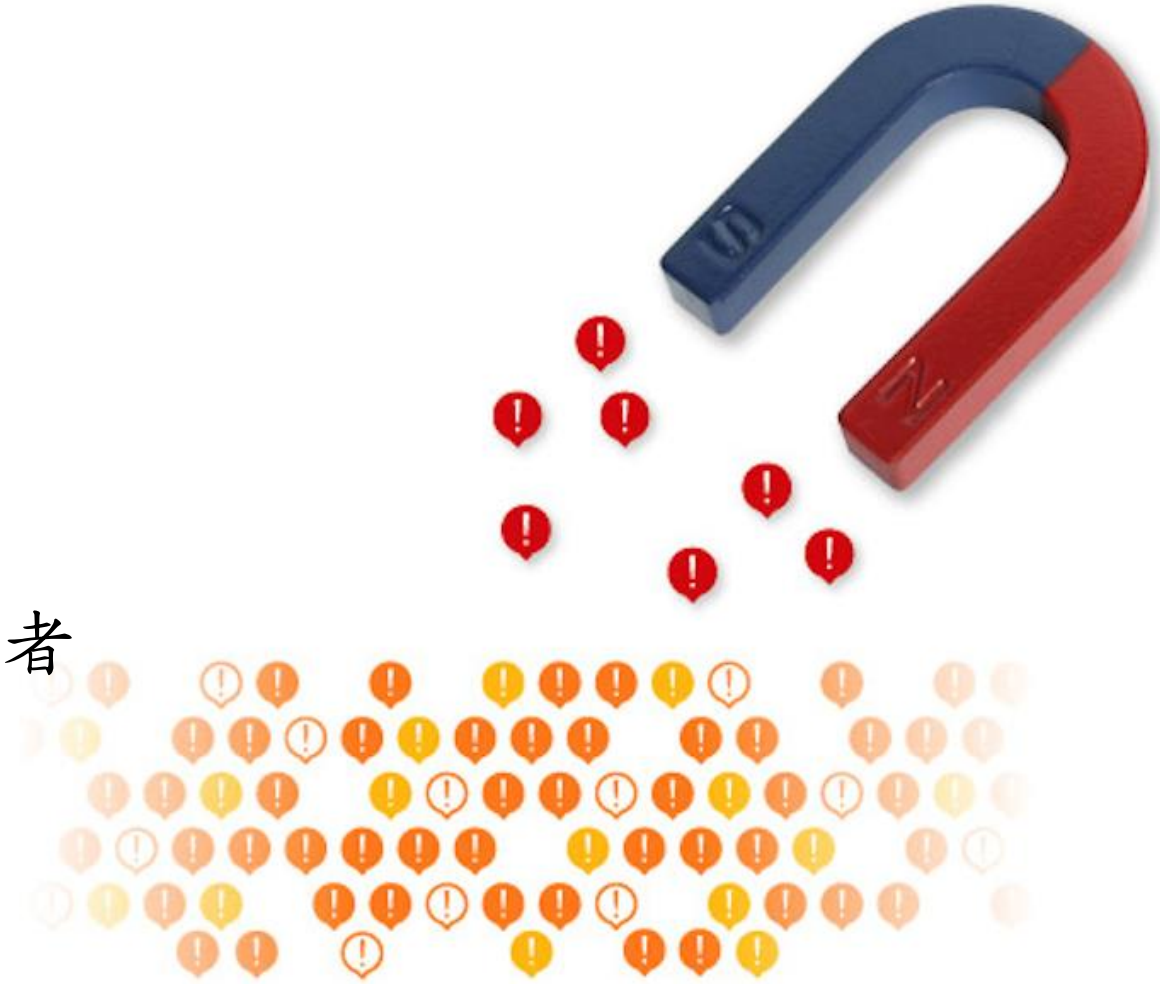
IMPERVA®

Attack Analytics可幫助您智慧化分析WAF安全事件

1. 收集WAF 的安全事件(Security Events)

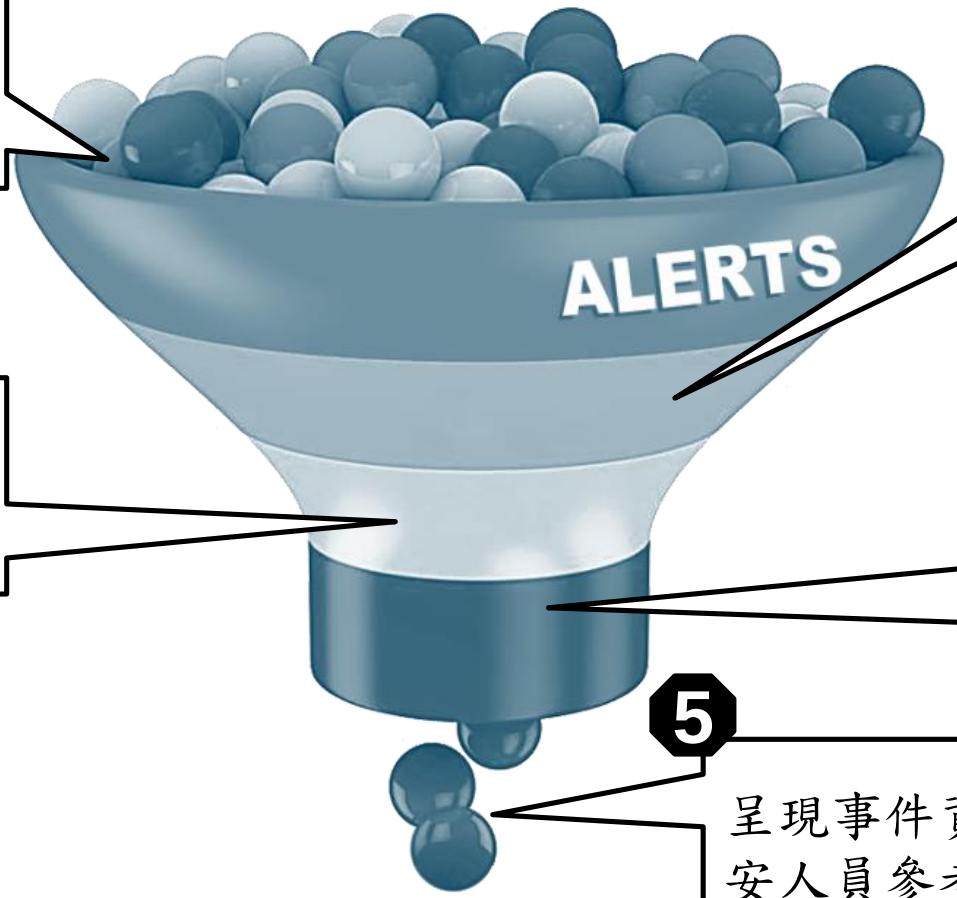
2. 事件排序及群組化

3. 經由智慧化的分析列出最需要管理者注意的極少量高價值安全事件。

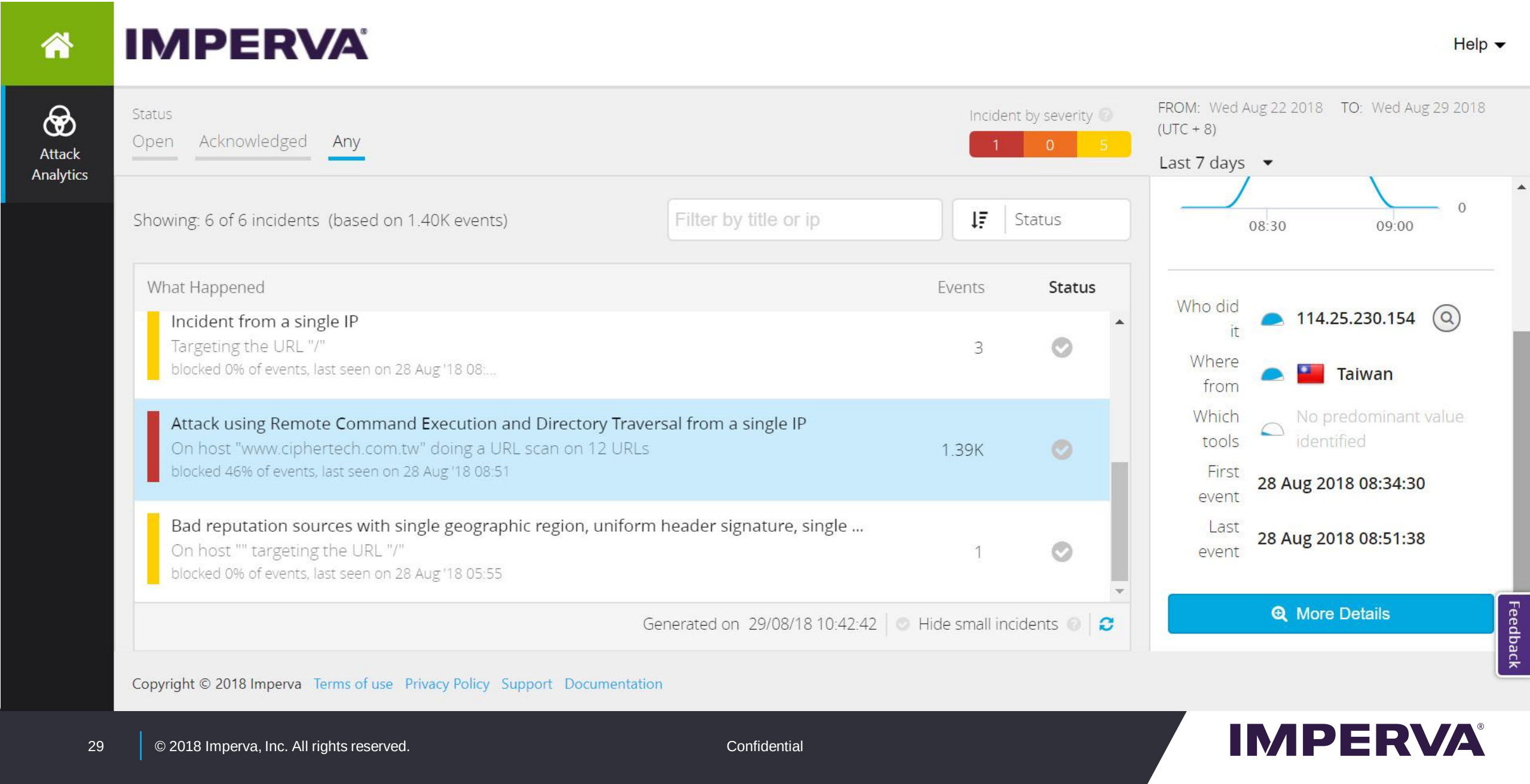


How it works

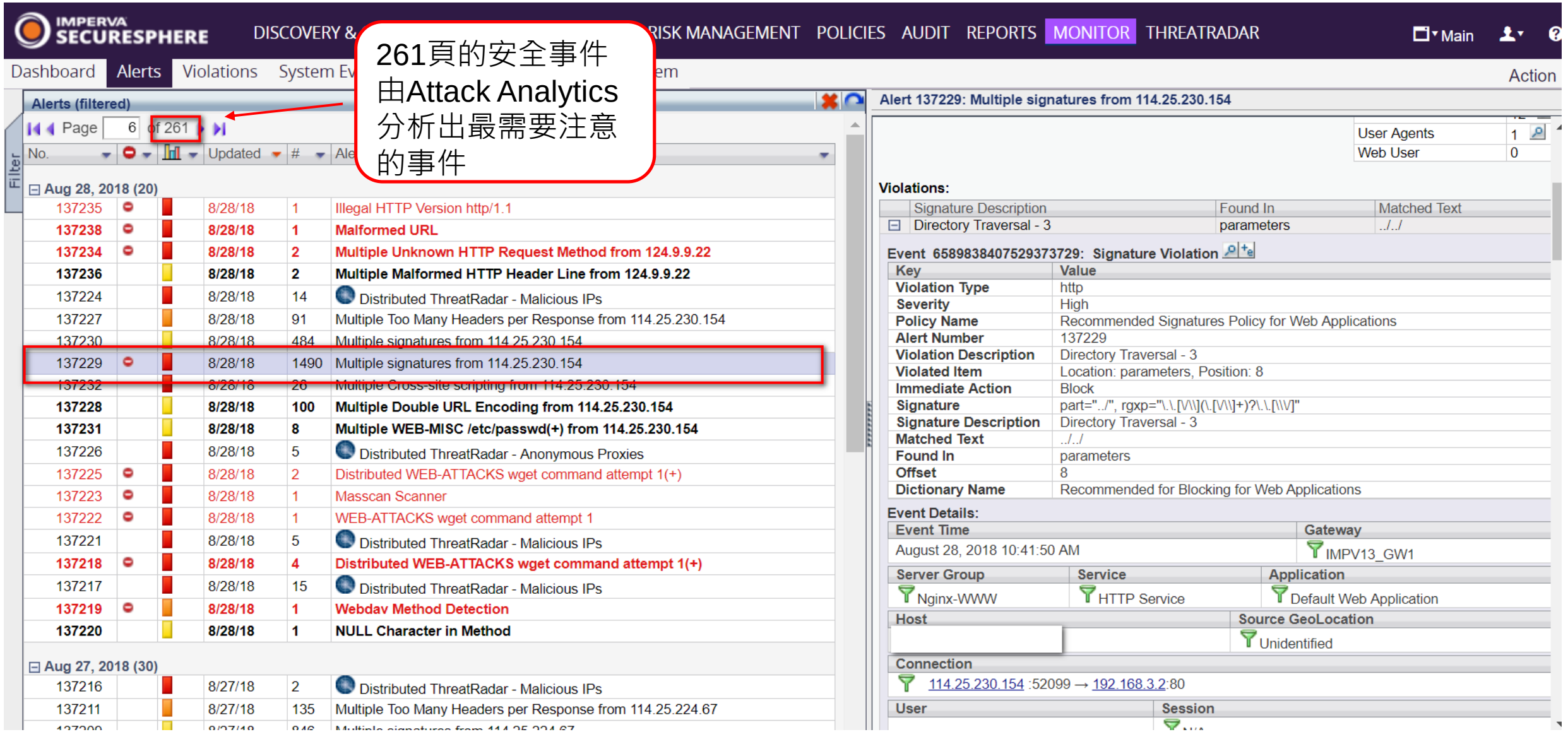
1. 收集WAF的事件資訊(On-Prem. or Cloud)
2. 機器學習與人工智慧分析事件，找出最需要關注的事件
3. 整合Web攻擊資料庫，增加事件解讀資訊
4. 確定事件優先等級
5. 呈現事件資訊以供資安人員參考與因應



IMPERVA®



IMPERVA



IMPERVA

Imperva Attack Analytics

Before	After
25% of websites monitored	**100%** of websites monitored
2.00 FTE	**2.00** FTE
109 K alerts per day	**64** narratives per day
2% (1,000) of alerts investigated	**100%** (64) of narratives investigated
0 significant incidents discovered	**2** significant narratives discovered

CASE STUDY: Crypto Currency Company

RESULTS

4x more WAF traffic monitored and investigated

Same FTE

1700x reduction in rate of alerts

100x increase in alerts investigated

IMPERVA ATTACK ANALYTICS

IMPROVED EFFECTIVENESS OF APPLICATION SECURITY WITHOUT INCREASED LABOR COSTS

少即是多(Less is more)

Q&A

IMPERVA®