

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

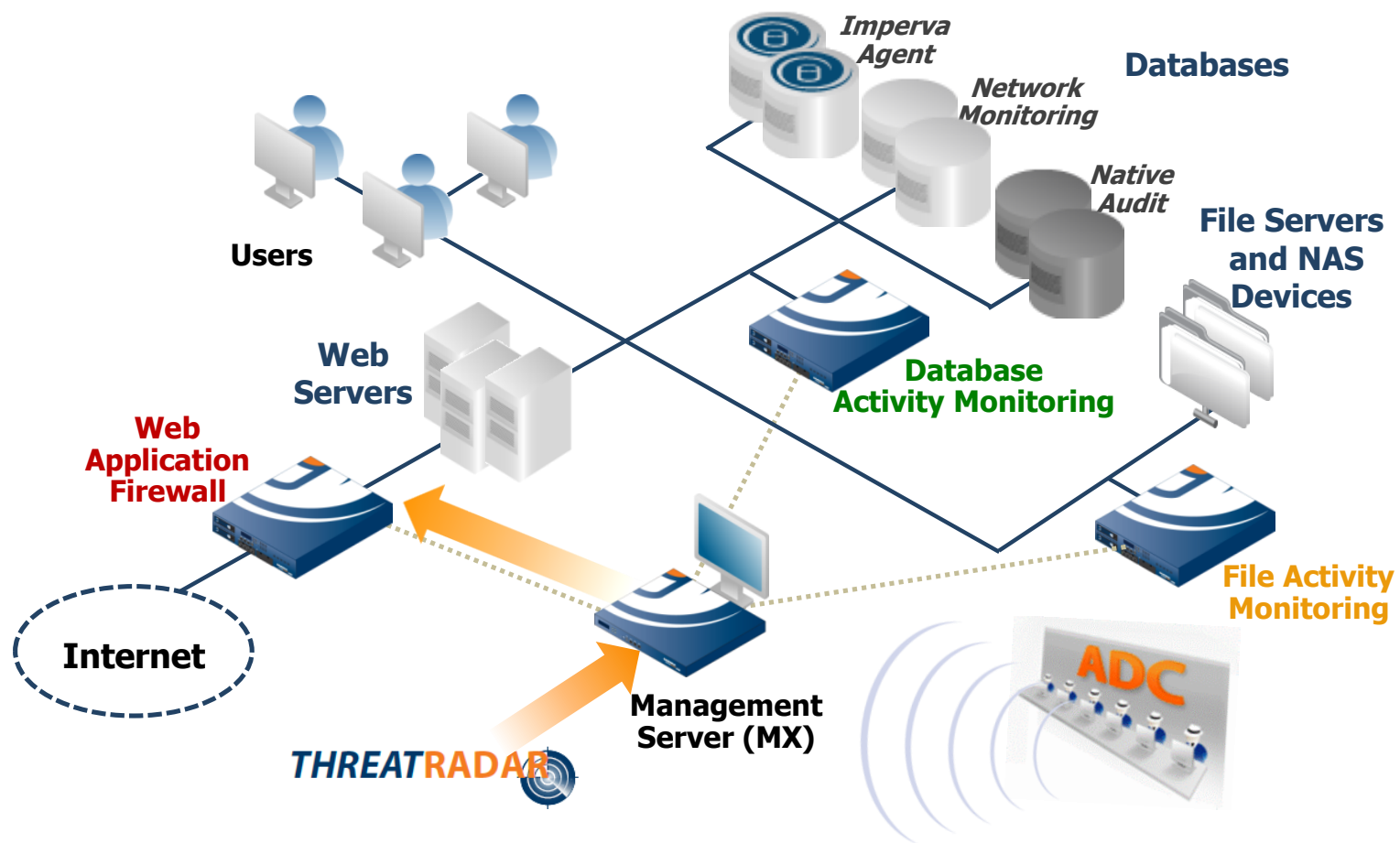
IMPERVA台灣資深技術顧問 范鴻志 Holmes Fan

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

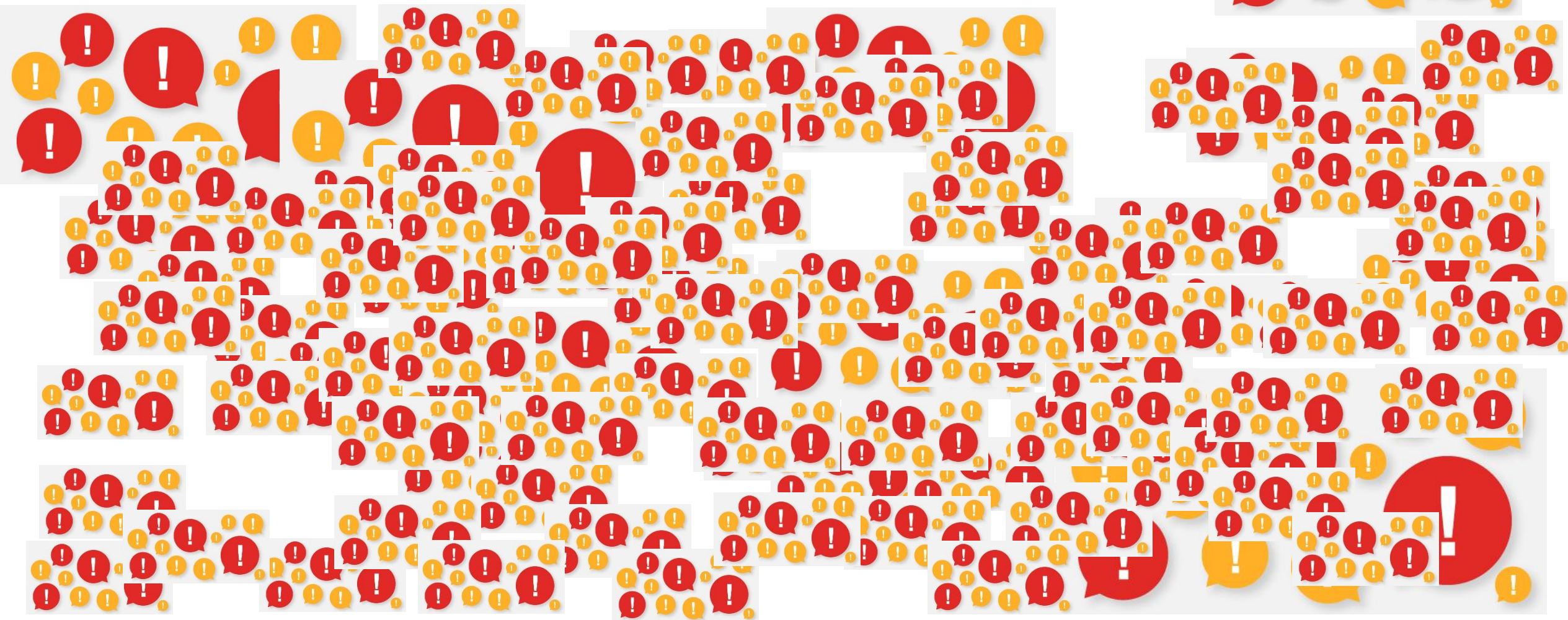
User大部分是資安訊息的被動接收者(Receiver)，少部分是傳遞者(Forwarder)

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

無以計數
的事件



極少量高價值
之事件



IMPERVA DAM可以幫您做到必須要做的資料庫稽核及安全

The screenshot displays the IMPERVA SECURESPHERE interface, which is divided into several sections for monitoring database security.

Left Panel: Audit Events

- Reported Period:** 03/06/2018, 00:00- 03/13/2018, 23:53 (7 Days, 23 hrs)
- Base Filter:** User is [sa]
- Filter:** Empty
- Select Columns:** Event Date and Time, Event ID, Source IP, User, Destination IP
- Table:** A list of audit events for MSSQL(137.45). The table includes columns for Event Date and Time, Event ID, Source IP, User, and Destination IP. The events are filtered for March 6, 2018, and show multiple attempts of unauthorized access.

Center Panel: Alerts

- Alerts (filtered):** A table showing alerts for March 6, 2018, and March 2, 2018. The table includes columns for No., Date, Time, and Alert Description. The alerts are filtered for March 6, 2018, and show multiple attempts of unauthorized access.
- Alert 192003: Unauthorized Host t470-172501 by holmes from 192.168.137.1**

Right Panel: Alert Details

- Alert 192003: Unauthorized Host t470-172501 by holmes from 192.168.137.1**
- Actions:** None
- Policy:** SQL Profile Policy
- Event 167503724555: Unauthorized Host**
- Event Details:** Event Time: March 2, 2018 6:08:39 PM, Gateway: v2500
- Server Group:** Windows 2012R2(137.45)
- Service:** MSSQL Service
- Application:** Default MsSql Application
- Connection:** 192.168.137.1:51303 → 192.168.137.45:1433
- Source of Activity:** Remote
- User:** holmes
- DB Application:** microsoft sql server management studio
- OS User:** 1470-
- OS Host:** 172501
- Affected Rows:** 0
- Response Size:** 0 Records
- Response Time:** 0 msec.
- Error Code:** 18456
- Error Message:** Login failed for user 'holmes'.

Bottom Panel: SQL Query

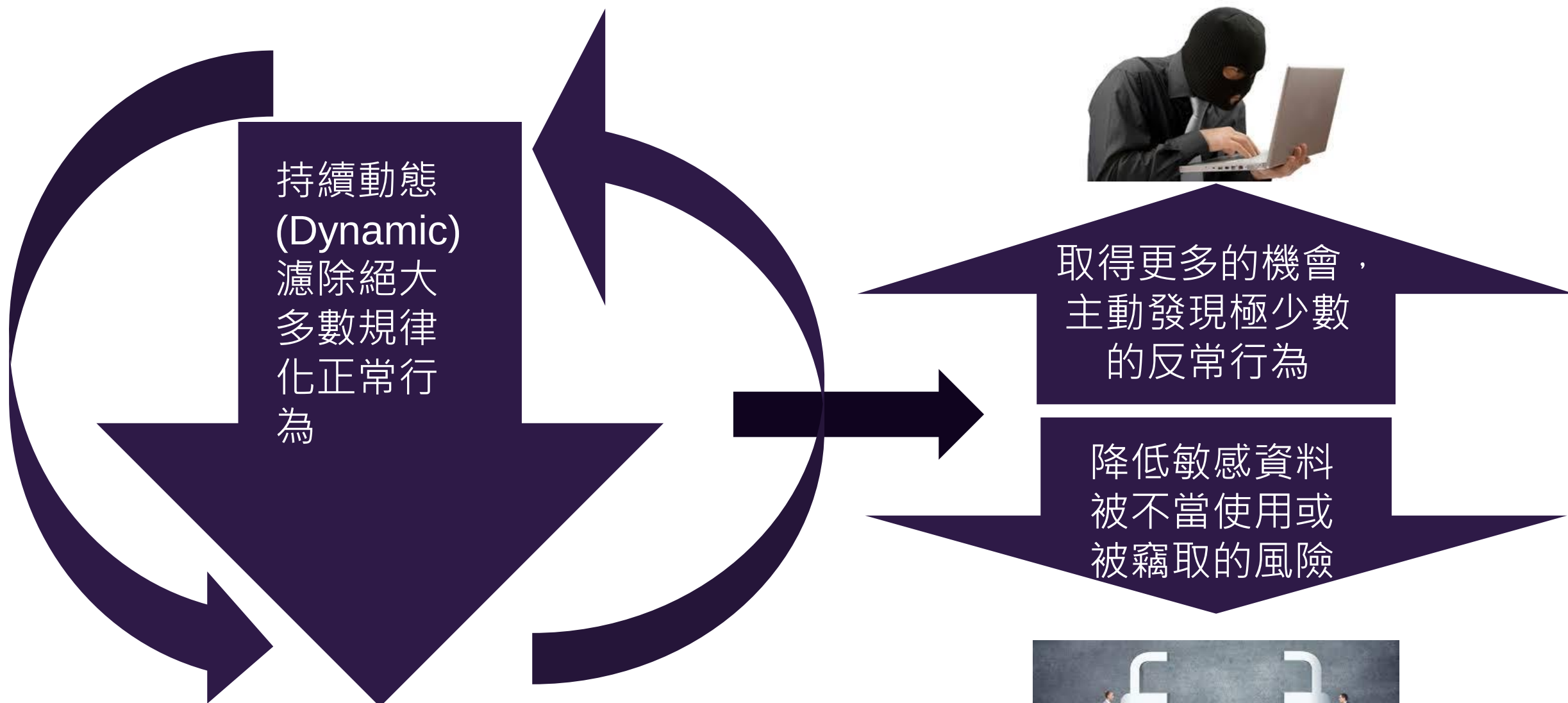
```
SELECT system_sql_modules, SELECT SCHEMA_NAME(sp.schema_id) AS [Schema], sp.name AS [Name], sp.object_id AS [ID], CAST(
SELECT sql_modules, SELECT SCHEMA_NAME(sp.schema_id) AS [Schema], sp.name AS [Name], sp.object_id AS [ID], CAST(
SELECT all_objects, SELECT SCHEMA_NAME(sp.schema_id) AS [Schema], sp.name AS [Name], sp.object_id AS [ID], CAST(
SELECT system_sql_modules, SELECT SCHEMA_NAME(udf.schema_id) AS [Schema], udf.name AS [Name], udf.object_id AS [ID], (cas
SELECT extended_properties, SELECT SCHEMA_NAME(udf.schema_id) AS [Schema], udf.name AS [Name], udf.object_id AS [ID], (cas
SELECT sql_modules, SELECT SCHEMA_NAME(udf.schema_id) AS [Schema], udf.name AS [Name], udf.object_id AS [ID], (cas
SELECT xml_schema_collections, SFI FCT SCHFMA NAME(udf.schema_id) AS [Schema], udf.name AS [Name], udf.object_id AS [ID], (cas
```


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



事件分析五個基本元素

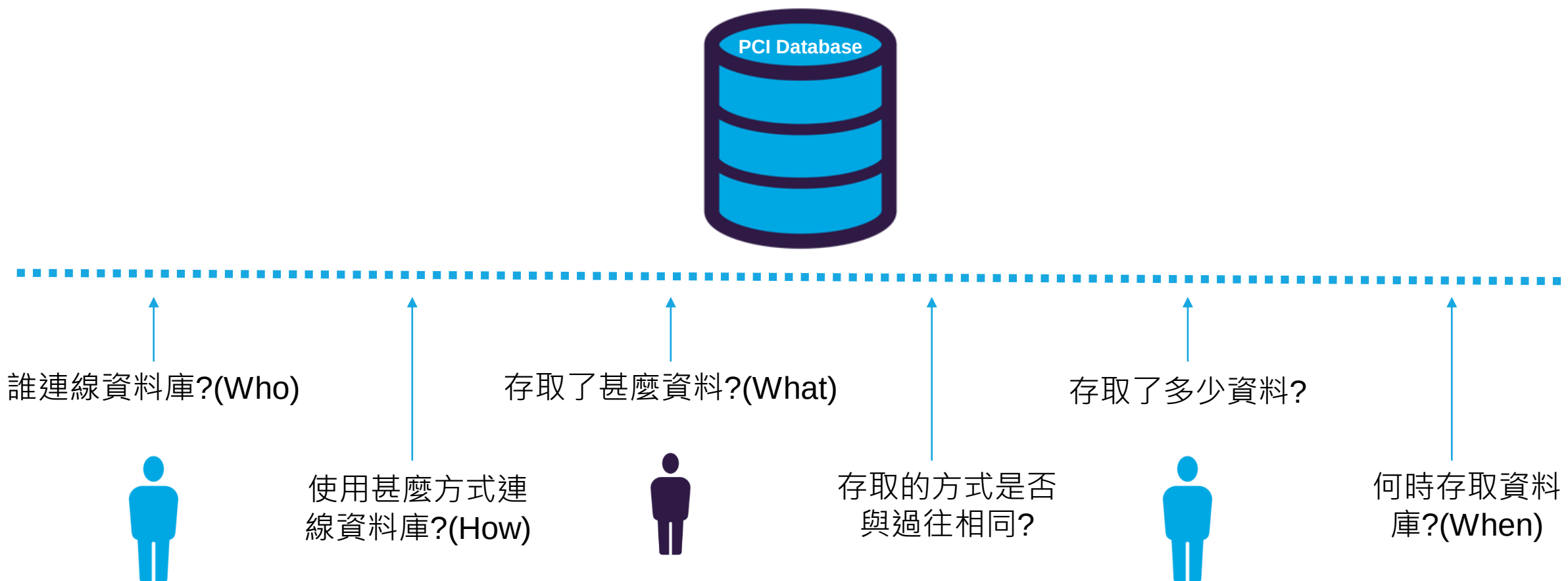
- ❖ 人
- ❖ 事
- ❖ 時
- ❖ 地
- ❖ 物

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



Behavior: 建立使用者存取資料庫的判斷基準線(Baseline)



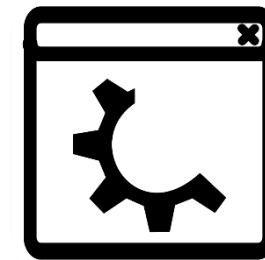
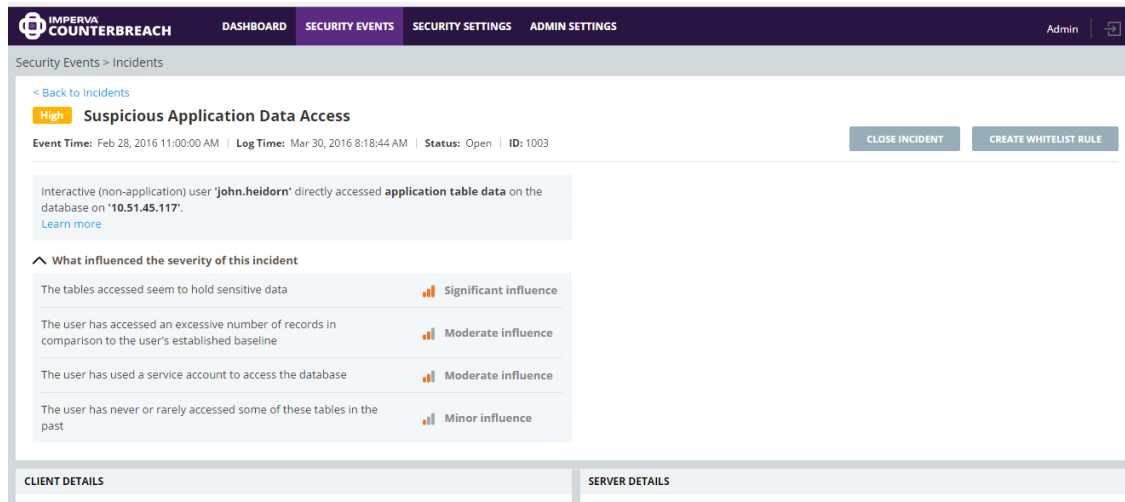
情境一 – Suspicious Application Data Access

(應用程式資料被其他user直接存取)

Detect

- Identify compromised, careless and malicious users

— Application Data Access

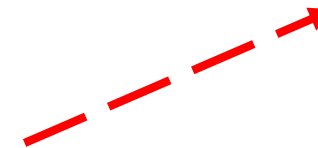


Application

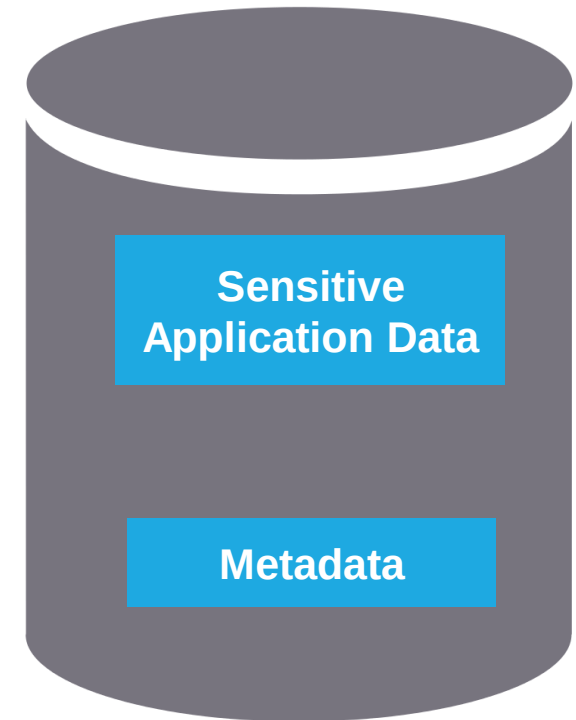


Interactive User (DBA)

Service Account



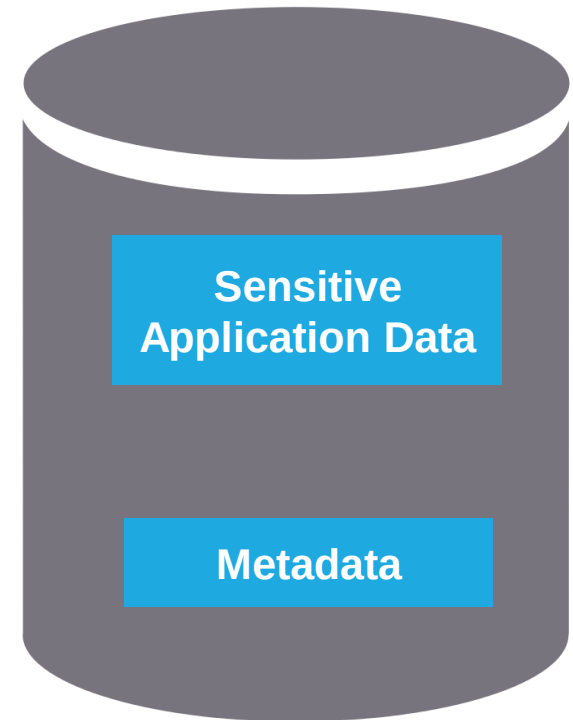
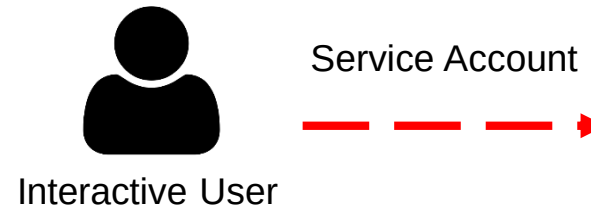
DB Account



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



IMPERVA
COUNTERBREACH

DASHBOARD

SECURITY EVENTS

SECURITY SETTINGS

ADMIN SETTINGS

Admin

Security Events > Incidents

7 OPEN

2 HIGH

CLOSE SELECTED

MANAGE WHITELIST RULES

Showing 1 - 7 of 7 Incidents | ☐ Show closed incidents (1,428) | Show incidents logged since:

All Time

 |

Filter Incidents

☐ SEVERITY ▾ TYPE

EVENT TIME

LOG TIME

STATUS

USER NAME

HOST

SOURCE IP

DESTINATION IP

☐

High

Suspicious Application Data Access

#1003

Interactive (non-application) user 'john.heidorn' directl...

Feb 28, 2016 11:00:00 AM

Mar 30, 2016 8:18:44 AM

Open

john.heidorn

win7x-john.h-desk

159.3.108.69

10.51.45.117

☐

High

Database Service Account Abuse

#1002

Interactive (non-application) user 'john.heidorn' logged...

Feb 28, 2016 11:00:00 AM

Mar 30, 2016 8:18:43 AM

Open

john.heidorn

win7x-john.h-desk

10.10.32.41

10.10.194.32

☐

Medium

Excessive Personal File Access

#1302

User 'mariam.harris' accessed an abnormally high num...

Jun 15, 2015 1:00:05 AM

Apr 05, 2016 1:30:34 AM

Open

mariam.harris

win7-harris.m

10.100.65.53

10.254.100.73

☐

Medium

Excessive Personal File Access

#1303

User 'nate.civian' accessed an abnormally high numbe...

Jun 15, 2015 1:00:05 AM

Apr 05, 2016 2:02:07 AM

Open

nate.civian

win7-nate.c

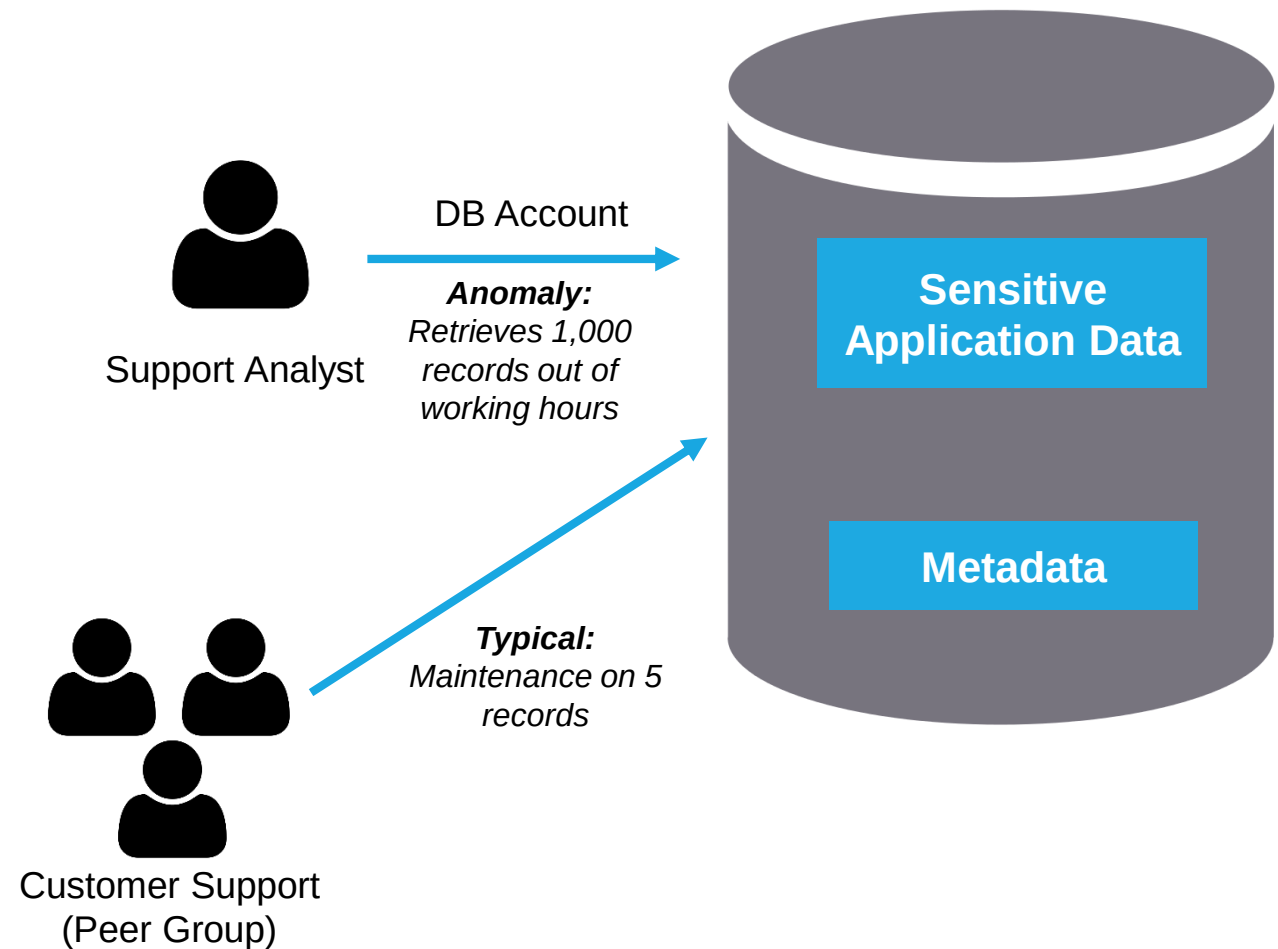
10.10.30.17

10.254.100.73

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



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**

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。



Attack
Analytics

Imperva Attack Analytics

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

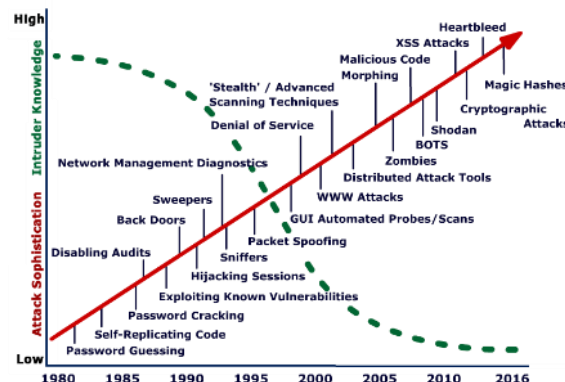
54%

因為龐大的安全事件
量而不知所措

Imperva Survey at RSA Security Conference 2018

[illegible]

攻擊手法不斷翻新
及
攻擊涵蓋面持續擴增



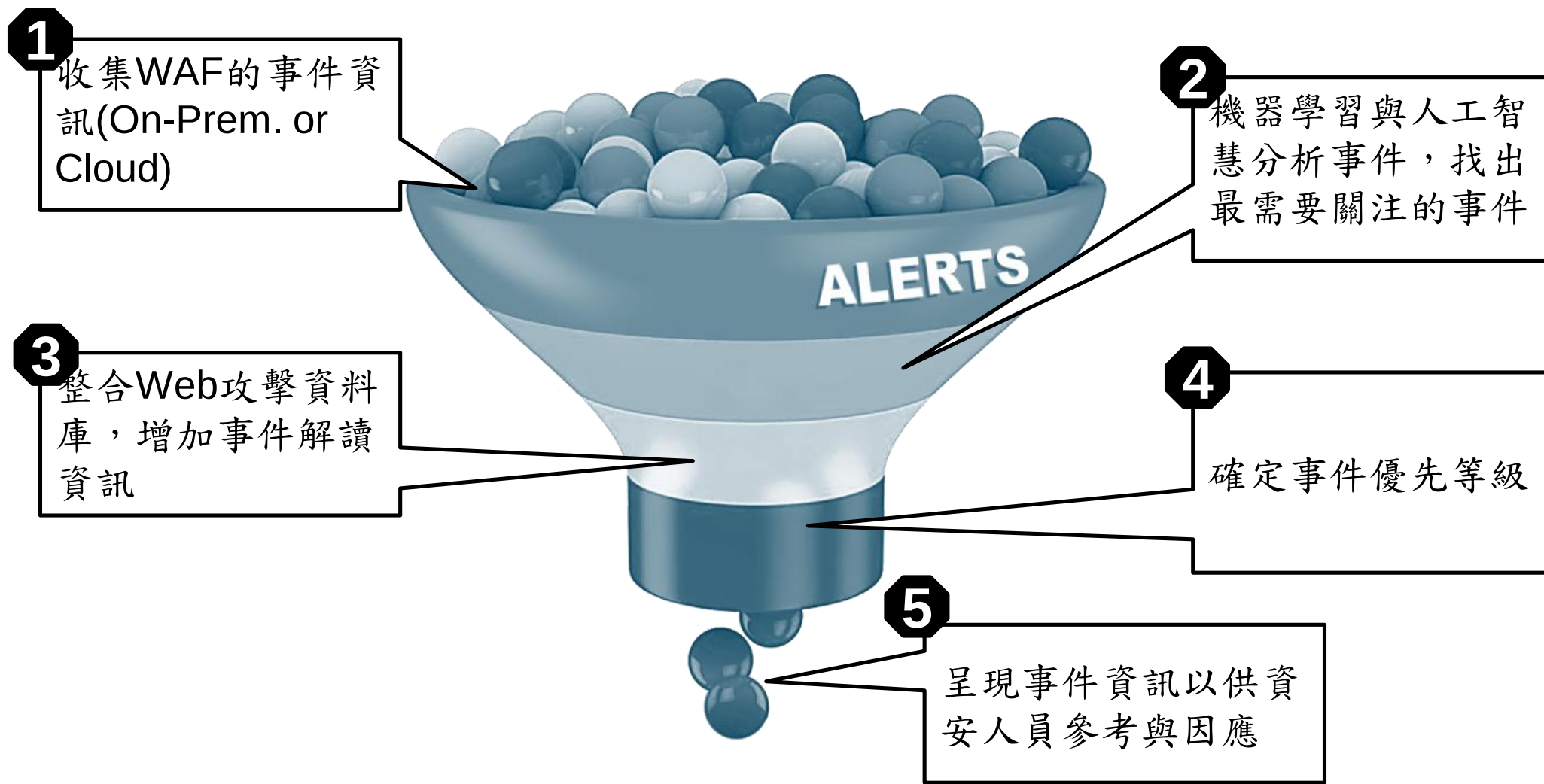
安全事件分析專業人員的缺乏

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





Status

Open

Acknowledged

Any

Incident by severity ?

1

0

5

FROM: Wed Aug 22 2018 TO: Wed Aug 29 2018
(UTC + 8)

Last 7 days ▼



Showing: 6 of 6 incidents (based on 1.40K events)

Filter by title or ip



Status

What Happened

Events

Status

Incident from a single IP

Targeting the URL "/"

blocked 0% of events, last seen on 28 Aug '18 08:...

3



Attack using Remote Command Execution and Directory Traversal from a single IP

On host "www.ciphertech.com.tw" doing a URL scan on 12 URLs

blocked 46% of events, last seen on 28 Aug '18 08:51

1.39K



Bad reputation sources with single geographic region, uniform header signature, single ...

On host "" targeting the URL "/"

blocked 0% of events, last seen on 28 Aug '18 05:55

1



Generated on 29/08/18 10:42:42 | ☒ Hide small incidents ?

Who did
it



114.25.230.154



Where
from



Taiwan

Which
tools



No predominant value
identified

First
event

28 Aug 2018 08:34:30

Last
event

28 Aug 2018 08:51:38

More Details

Feedback

IMPERVA

SECURESPHERE

DISCOVERY & ANALYTICS

RISK MANAGEMENT

POLICIES

AUDIT

REPORTS

MONITOR

THREATRADAR

Dashboard

Alerts

Violations

System Events

Alerts (filtered)

Page 6 of 261

Filter

No.

Updated

#

Alert

Aug 28, 2018 (20)

137235

8/28/18

1

Illegal HTTP Version http/1.1

137238

8/28/18

1

Malformed URL

137234

8/28/18

2

Multiple Unknown HTTP Request Method from 124.9.9.22

137236

8/28/18

2

Multiple Malformed HTTP Header Line from 124.9.9.22

137224

8/28/18

14

Distributed ThreatRadar - Malicious IPs

137227

8/28/18

91

Multiple Too Many Headers per Response from 114.25.230.154

137230

8/28/18

484

Multiple signatures from 114.25.230.154

137229

8/28/18

1490

Multiple signatures from 114.25.230.154

137232

8/28/18

26

Multiple Cross-site scripting from 114.25.230.154

137228

8/28/18

100

Multiple Double URL Encoding from 114.25.230.154

137231

8/28/18

8

Multiple WEB-MISC /etc/passwd(+) from 114.25.230.154

137226

8/28/18

5

Distributed ThreatRadar - Anonymous Proxies

137225

8/28/18

2

Distributed WEB-ATTACKS wget command attempt 1(+)

137223

8/28/18

1

Masscan Scanner

137222

8/28/18

1

WEB-ATTACKS wget command attempt 1

137221

8/28/18

5

Distributed ThreatRadar - Malicious IPs

137218

8/28/18

4

Distributed WEB-ATTACKS wget command attempt 1(+)

137217

8/28/18

15

Distributed ThreatRadar - Malicious IPs

137219

8/28/18

1

Webdav Method Detection

137220

8/28/18

1

NULL Character in Method

Aug 27, 2018 (30)

137216

8/27/18

2

Distributed ThreatRadar - Malicious IPs

137211

8/27/18

135

Multiple Too Many Headers per Response from 114.25.224.67

137200

8/27/18

848

Multiple signatures from 114.25.224.67

261頁的安全事件
由Attack Analytics
分析出最需要注意
的事件

Alert 137229: Multiple signatures from 114.25.230.154

User Agents

Web User

1

0

Violations:

Signature Description

Found In

Matched Text

Directory Traversal - 3

parameters

../..

Event 6589838407529373729: Signature Violation

Key

Value

Violation Type

http

Severity

High

Policy Name

Recommended Signatures Policy for Web Applications

Alert Number

137229

Violation Description

Directory Traversal - 3

Violated Item

Location: parameters, Position: 8

Immediate Action

Block

Signature

part="..", rgxp="\.[\W](\.[\W]+)?\.[\W]"

Signature Description

Directory Traversal - 3

Matched Text

../..

Found In

parameters

Offset

8

Dictionary Name

Recommended for Blocking for Web Applications

Event Details:

Event Time

Gateway

August 28, 2018 10:41:50 AM

IMPV13_GW1

Server Group

Service

Application

Nginx-WWW

HTTP Service

Default Web Application

Host

Source GeoLocation

Unidentified

Connection

114.25.230.154 :52099 → 192.168.3.2:80

User

Session

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®