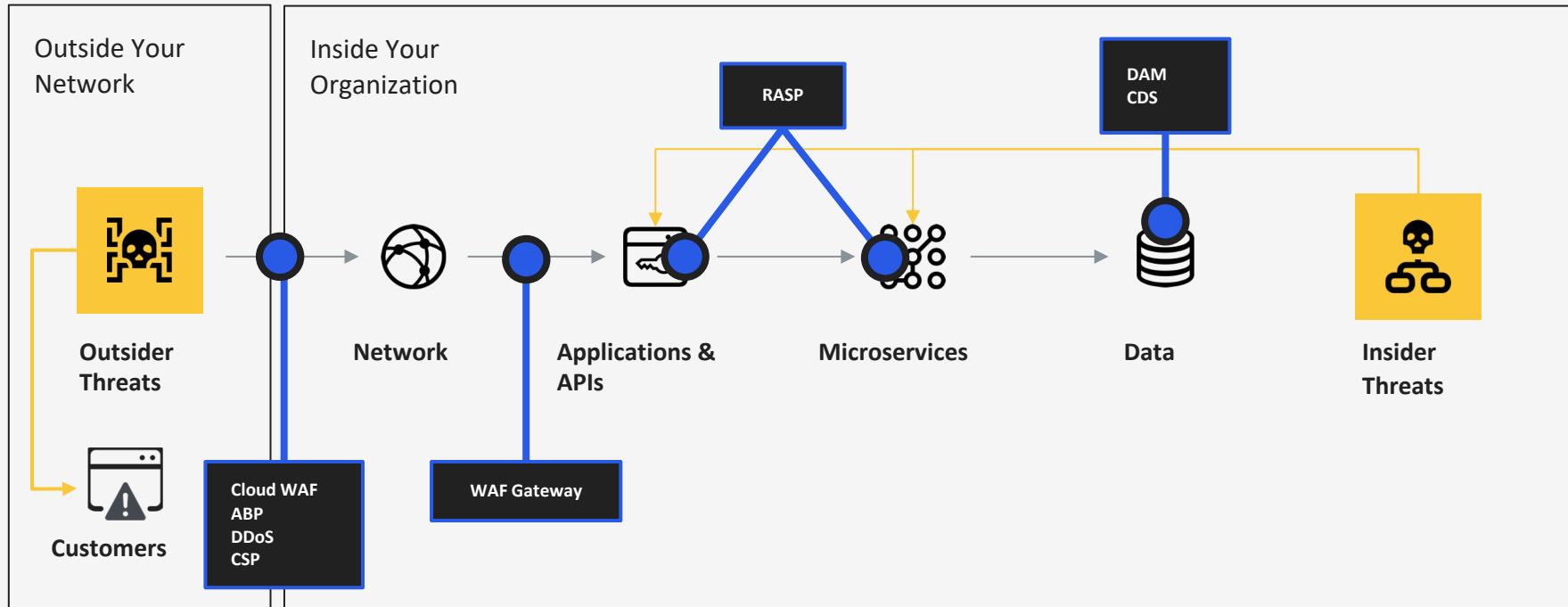




面對快速的變化與威脅，
需要全方位的防護來因應

范鴻志 Holmes Fan

Imperva對資料的全方位防禦



imperva 對資料的全方位防禦(Edge to End Protection)

邊境(境外，跨域)防禦
Edge Security



Distributed Denial
of Service
DDoS



Content Delivery
Network
CDN

應用程式安全
Application Security



Web Application
Firewall
WAF



Advanced Bot
Protection
ABP



Runtime Application
Self-Protection
RASP



Attack
Analytics
AA

資料庫安全
Data Security



Database Activity
Monitoring
DAM



Cloud Data
Security
CDS



Discovery &
Assessment
DAS



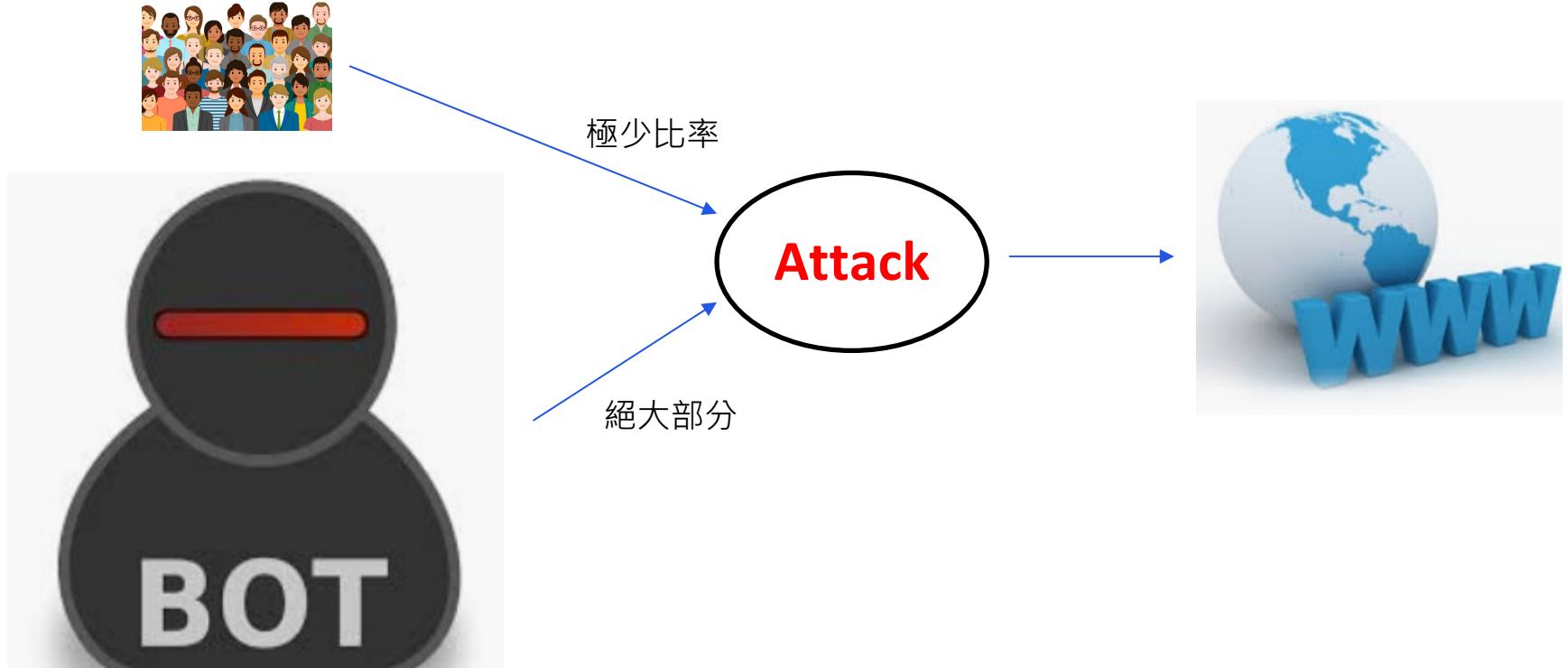
Data Risk
Analytics
DRA



Advanced Bot Protection (ABP)



絕大部分對Web的攻擊來自機器人連線



不是所有的機器人連線都是不好的

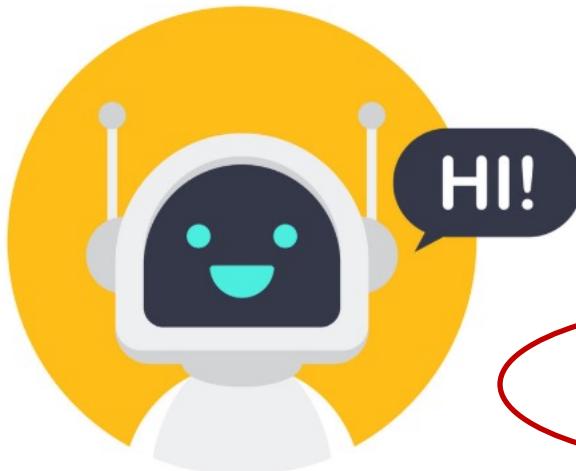
Google

yahoo!

Bing

Baidu

facebook



嗨，我是好的
機器人連線

我可以幫助您增加您公司網
站的曝光度，進而幫助您增
加商機

壞機器人攻擊極可能傷害企業的營運



Web被爬網(網站內容與價格資訊)

- 營收損失(競爭者得利)
- 銷售及促銷策略被立即複製
- 被搜尋引擎負評
- 網頁被假造，造成客戶資料被竊取



營運成本倍增

- 需要花費大量人力及時間處理網站服務被影響之問題
- 因為被事件影響，極可能因思緒不清做出錯誤決策而造成不必要的成本付出
- 員工士氣及鬥志受影響



網站服務變慢甚至掛點

- 營收損失
- 客訴狂增
- 商譽損失

我要如何知道是這個機器人連線是好的還是不好的？



我覺得你是好的

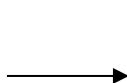
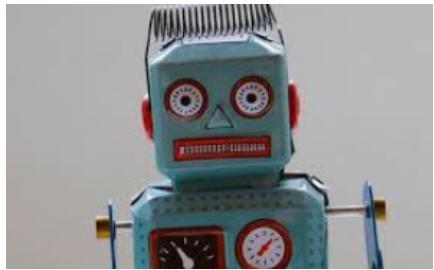
我認為你是不好的

X

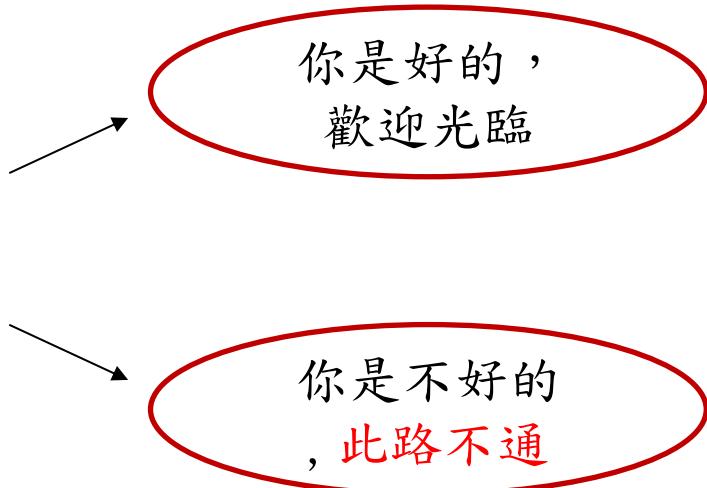
X

營收損失
商譽損失
...

別擔心，Imperva可以幫助您



imperva
Bot Management

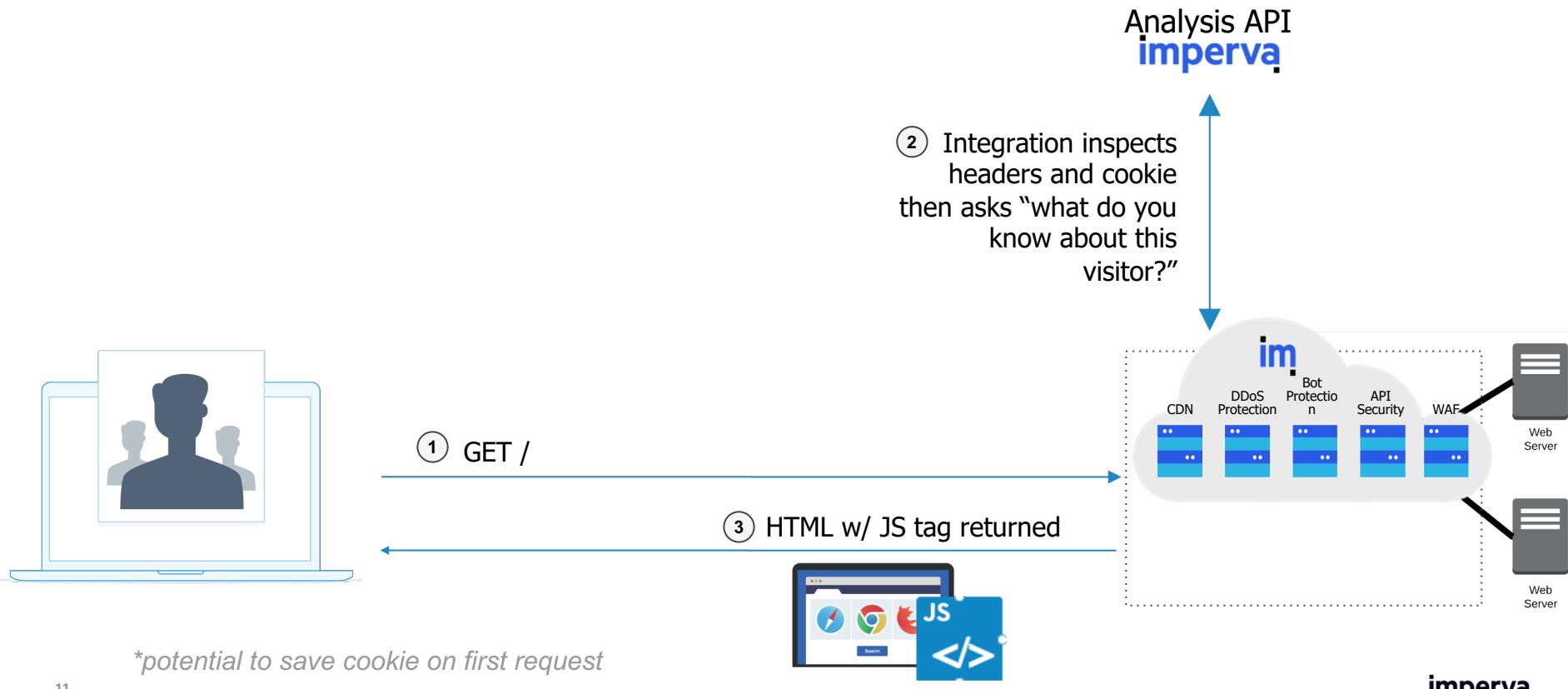


與連線來源詢答，來確認來源是否是機器人連線？Client Side Interrogation
Validates the browser and determines “are they human?”

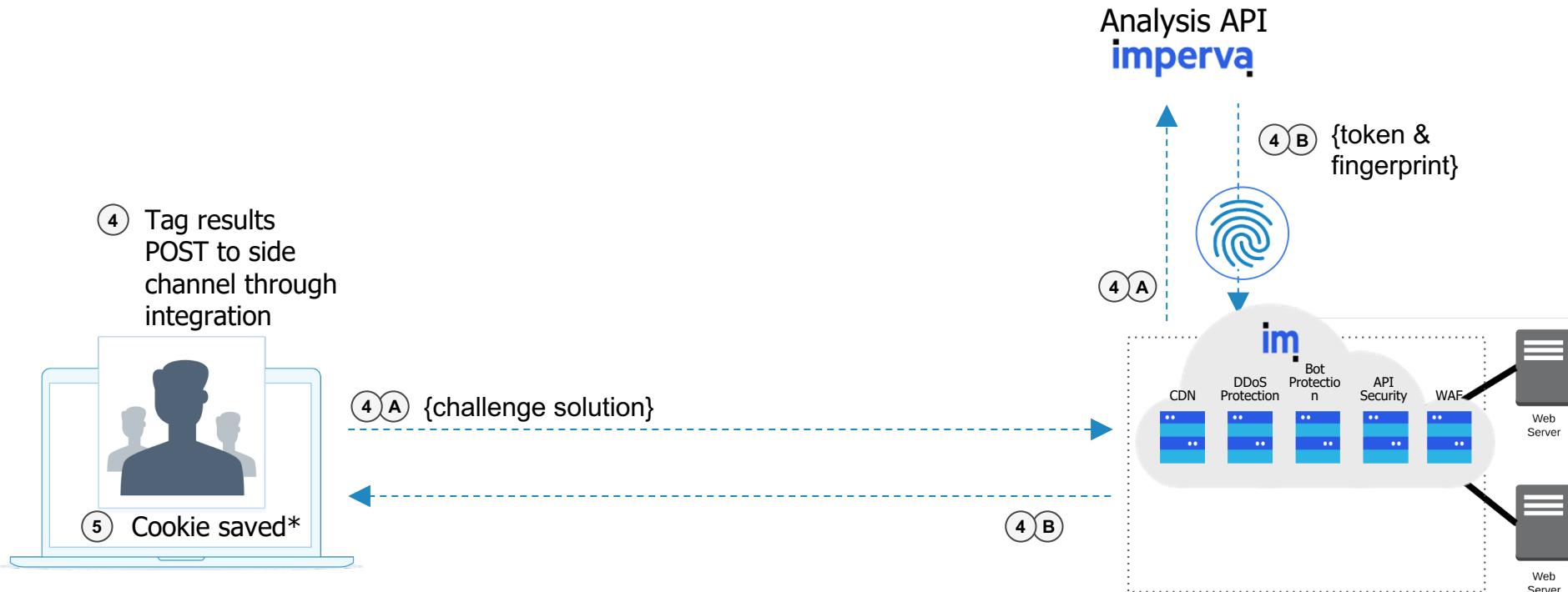
- Browser validation
 - Javascript engine
 - CSS Rendering
 - Request threading
- Device validation
 - Peripheral detection
 - Hardware identification (video, sound, network)
 - Battery, orientation, gyroscope



Connector High Level Diagram - Page GET



Connector High Level Diagram - JS POST



*potential to save cookie on first request



Data Risk Analytics (DRA)



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 web interface. At the top, there are two navigation bars: a blue one for 'DISCOVERY & CLASSIFICATION', 'SETUP', and 'PROFILE' on the left, and a purple one for 'MONITOR' and 'THREATRADAR' on the right. Below these are tabs for 'Dashboard', 'DB Audit Data', 'Directory Services Audit Data', and 'File Audit Data'. The main content area shows 'Audit Events' for 'MSSQL(137.45) Audit Policy - Audit Events'. It includes a 'Reported Period' from 03/06/2018 to 03/13/2018, a 'Base Filter' for 'User is [sa]', and a 'Filter' set to 'Empty'. A 'Select Columns' dropdown is open. The log table lists events from March 6, 2018, to March 10, 2018, with columns for 'Event Date and Time', 'Event ID', 'Source IP', 'User', and 'Destination IP'. Specific events include multiple logins from 192.168.137.1 and unauthorized access from host 172.50.1. The right side of the interface shows a detailed view of an alert for 'Unauthorized Host t470-172501 by holmes from 192.168.137.1' on March 6, 2018, at 08:39 PM. The alert details include the policy name 'SQL Profile Policy', the event number '167503724555', and the violation description 'Unauthorized Host t470-172501 by holmes from 192.168.137.1'. It also shows the connection details: source IP 192.168.137.1, user holmes, and destination IP 172.50.1.45. The 'Error Message' field indicates 'Login failed for user 'holmes''. The bottom right corner features the Imperva logo.

哇…，巨量的稽核資料，要如何找出極少量的異常行為？

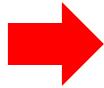


大海撈針

資料庫稽核是必要工作，但每日留存的資料量有如巨大冰山不理它，反正有保存，有需要再查不，上面的想法有點消極，我要從中找出反常行為，積極的預防資安事件，但....

正常行為高達所有行為的99.99.....，要想從中找尋極少量的反常行為猶如

如果……



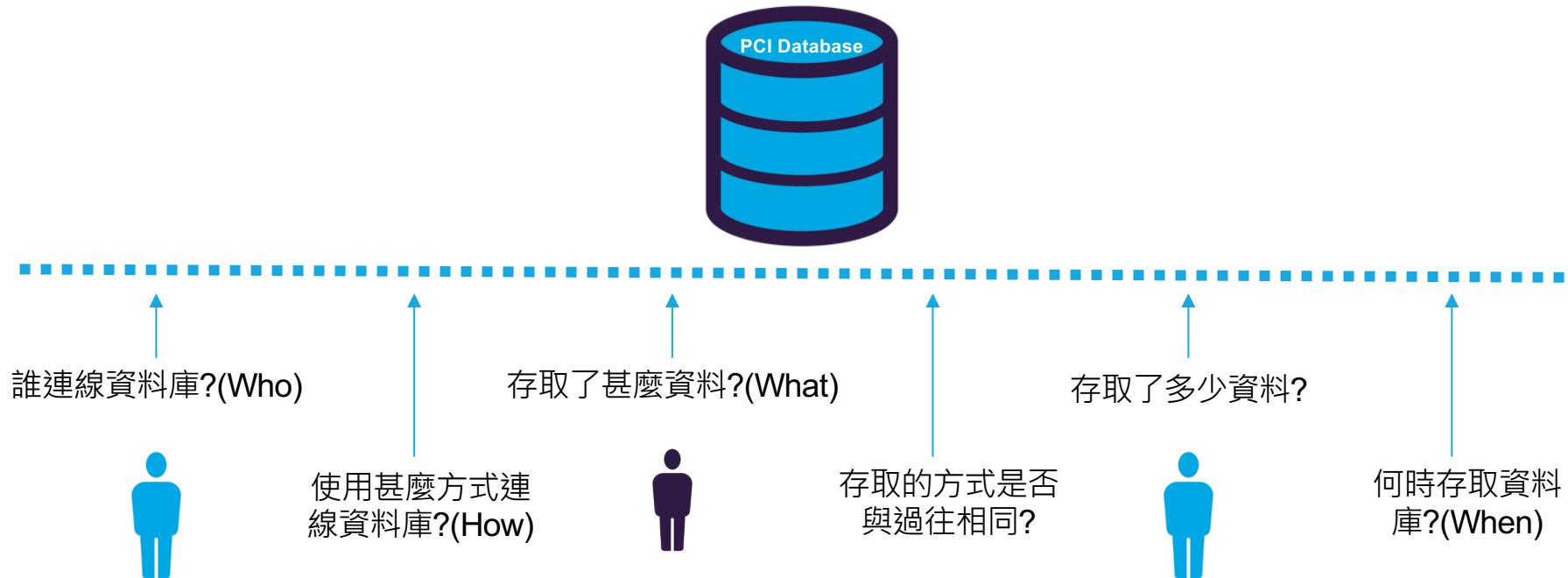
如果可將巨大的
冰山，濃縮成小
小的冰塊，那就
把不可能變成可
能

但要如何達到？

Imperva Data Risk Analytics 可幫助您從巨量的資料中發掘出異於常規的行為



Behavior: 建立使用者存取資料庫的判斷基準線(Baseline)



High

Suspicious Application Data Access



Event Time: Mar 3, 2017 10:00:00 PM | Status: Open | ID: 1148

Client Details



Information Technology
Application Support Engineer
Application Support Engineer

Host: [View details](#)
IP Address: [View details](#)
Source Application: [Interactive Tool](#)
Source Application: microsoft sql server management studio - query

Server Details



Mssql Server

DB User:
DB Name:

INCIDENT DESCRIPTION

John was identified as directly accessing business data (cc info) that should normally only be accessed via an application.

DB OPERATIONS (7)

 SEARCH

DB NAME	DB USER	SCHEMA	TABLE/STORED PROCEDURE	TYPE	CONTENT TYPE ▾	OPERATION	NO. OF QUERIES	TOTAL NO. OF RECORDS
db_gen001	sa_gen		client	table	SENSITIVE APPLICATION CONTENT	select	1	1
db_gen001	sa_gen		clientcreditcard	table	SENSITIVE APPLICATION CONTENT	select	1	2
db_gen001	sa_gen		clientcreditcard	table	SENSITIVE APPLICATION CONTENT	update	1	1

High

Excessive Database Record Access

☆ | Event Time: Mar 6, 2017 11:00:00 AM | Status: Open | ID: 1169

Client Details



Principal Developer

Host:

IP Address:

Source Application:

microsoft sql server
management studio
- query

User Endpoint

Interactive Tool

Server Details



MsSql Server

DB User:

DB Name:

Personal Account

INCIDENT DESCRIPTION

Laura retrieves an excess of 11.6 million records using 'microsoft sql server management studio' from a production database which is abnormally high. Usually two specific applications would access these records directly.

11688581 Records accessed from 1 table | 1 Operation performed on this DB server

DB OPERATIONS (1)							
DB NAME	DB USER	SCHEMA	TABLE/STORED PROCEDURE	TYPE	CONTENT TYPE	OPERATION	NO. OF QUERIES
		dbo	bet	table	SENSITIVE APPLICATION CONTENT	select	2 11,688,581

Imperva DRA可以幫助您

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 Data Risk Analytics)，達到最有效之資料庫使用行為**風險分析**、
統計與管控。

impervä

Thank You!

