



東海大學 IBM Guardium使用經驗分享

楊朝棟

東海大學 資訊工程學系 終身特聘教授

圖書暨資訊處 圖資長

<https://ithu.tw/cty>

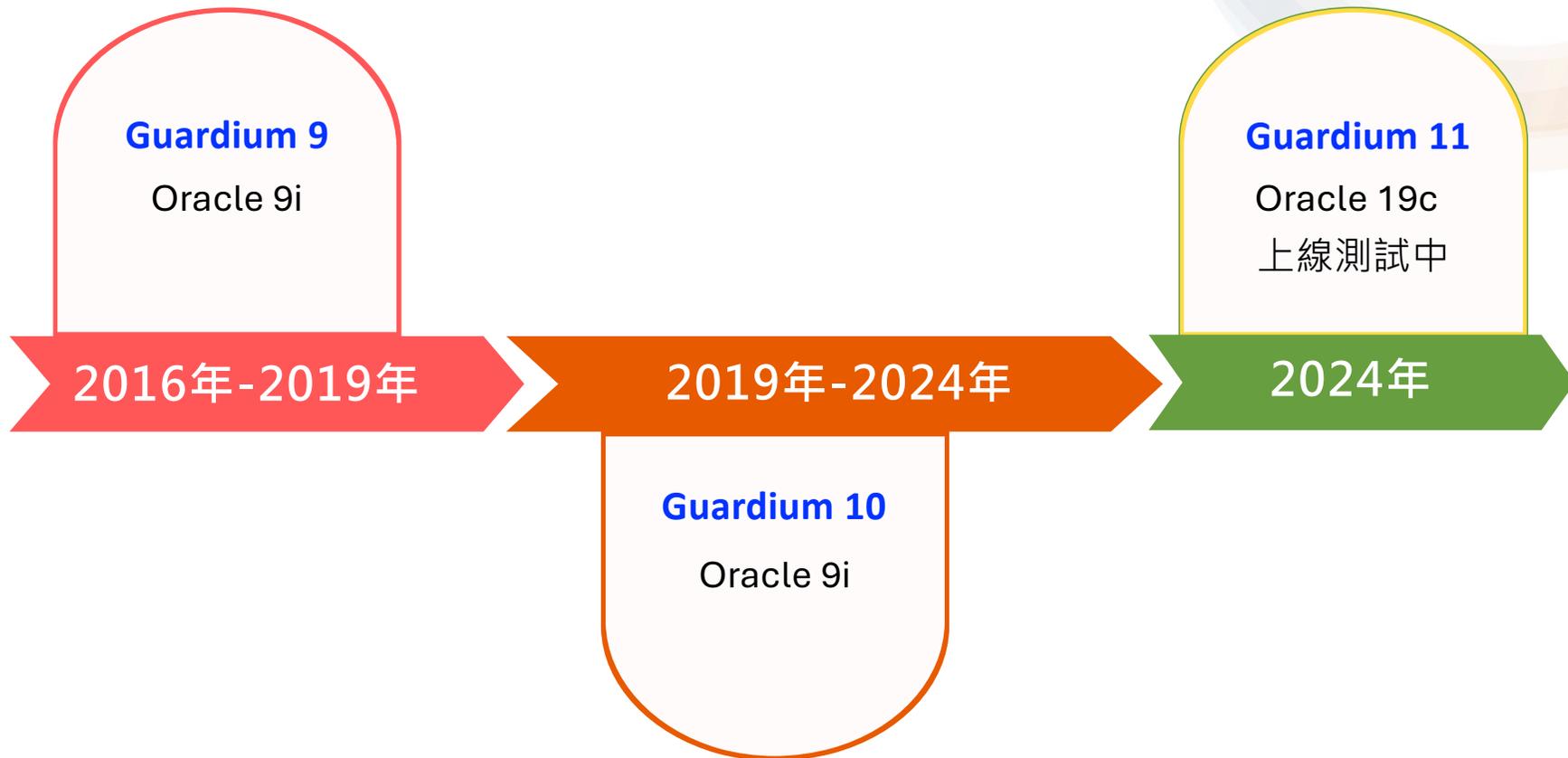


大綱

- 東海大學Guardium使用歷程
- 東海大學Guardium架構
- Guardium的優點
- 東海大學Guardium的實際應用
 - 自訂報表，找出不可否認的證據
 - 責任分工，加強監控
 - 實際應用情境分享



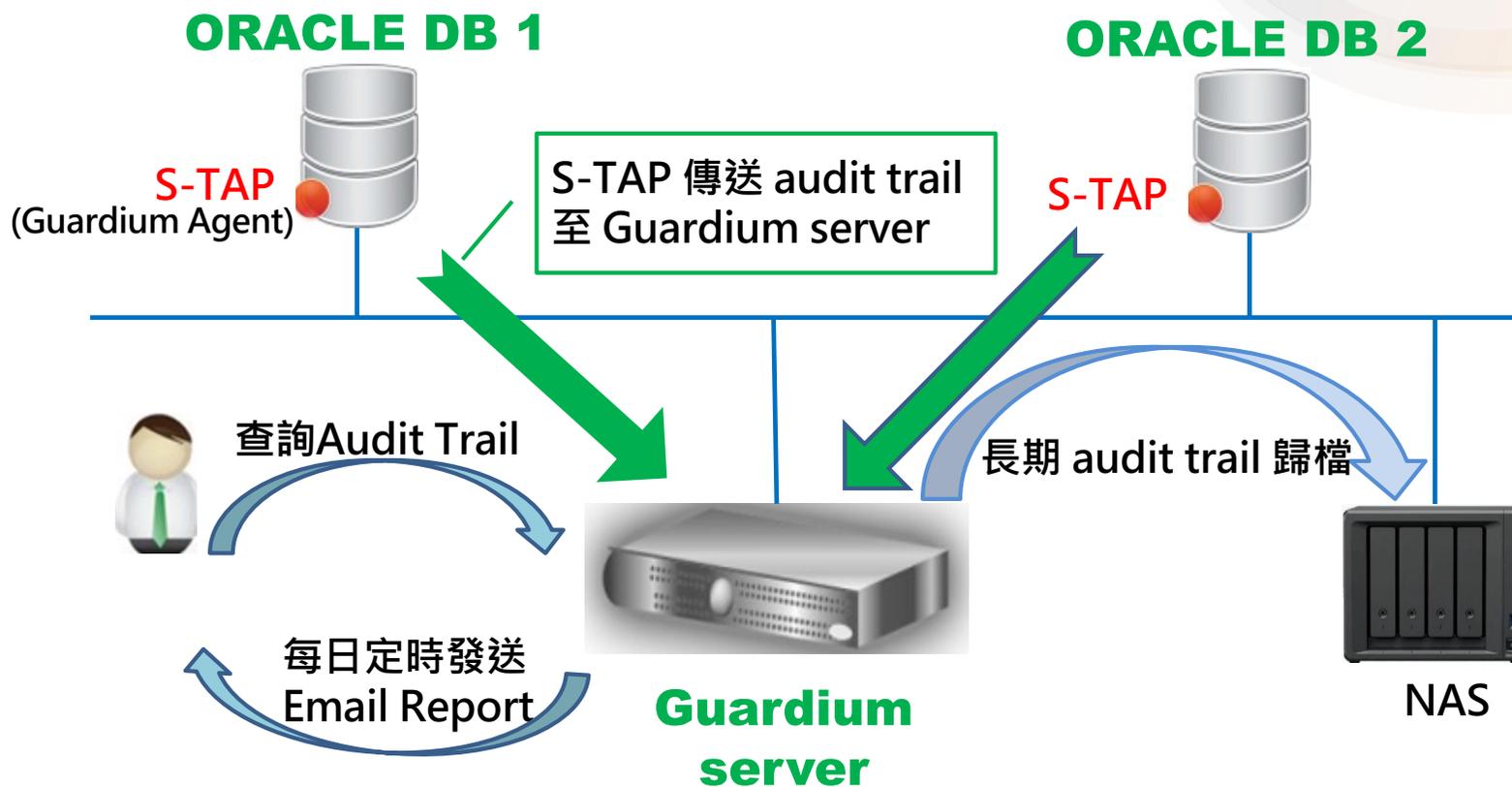
東海大學Guardium使用歷程





東海大學Guardium架構

凡走過必留痕跡





Guardium的優點



獨立監控

Guardium 有獨立數據庫儲存取數據，比起資料庫內建的AUDIT功能，更能確保監控數據的**不可否認性**。



安全合規

Guardium 提供實時監控，並遵守各種合規標準，使學校能更輕鬆地應對嚴格的資安法規要求。



數據加密與遮蔽技術

Guardium具備數據加密和遮蔽功能，確保敏感數據在儲存和傳輸過程中都能得到有效的保護，防止數據在傳輸過程中洩露。



Guardium的優點



提供內建檢核報表

Guardium 提供自動化的合規報告功能，也可協助生成所需的報表，以應對審計要求。

The screenshot displays the IBM Guardium web interface. The top navigation bar shows 'IBM Guardium' and the time '14:53'. A left sidebar contains menu items: Welcome, Setup, Manage, Discover, Harden, Investigate, and Protect. The 'Manage' section is expanded, showing options like 'Admin Users Login', 'Application Objects Summary', 'Audit Process Log', 'Configuration Change History', 'Detailed Enterprise S-TAP View', 'Dropped Requests', 'Enterprise S-TAP association history', 'Groups Usage Report', 'IMS Checkpoint Results', and 'Inactive Inspection Engines'. A modal window titled 'Manage' is open, displaying a table of session data for the date '4-09-23 14:51:34'. The table has columns for 'DB User Name', 'Source Program', 'Session Start', and 'Count of Sessions'.

DB User Name	Source Program	Session Start	Count of Sessions
SYS	RMAN	2024-09-23 03:00:02	3
SYS	RMAN	2024-09-23 03:00:03	3
SYS	SQLPLUS@WEBDB	2024-09-23 03:03:48	2
SYS	SQLPLUS@WEBDB	2024-09-23 03:04:29	1
SYS	SQLPLUS@WEBDB	2024-09-23 03:12:48	2
SYS	SQLPLUS@WEBDB	2024-09-23 03:12:49	1
SYS	RMAN	2024-09-23 02:42:20	5
SYS	RMAN	2024-09-23 02:42:21	1



東海大學Guardium的實際應用



只選擇重要
物件紀錄

優點：可以留存線上資料
的天數多，查詢速度快

缺點：可能遺漏重要物件



全都錄
凡走過必留痕跡



優點：可以查到任何做過的
指令、來源IP、使用帳號、
執行的工具或程式.....

缺點：資料量多，線上資料
可留存的天數少，查詢速度
慢



自訂監控報表，最想監控的是什麼？

學生成績

學生選課

Failed
login資訊

DB帳號的
Session
連線數量

學生、教職員、
校友敏感個資



駭客喜歡
用的工具
與Table



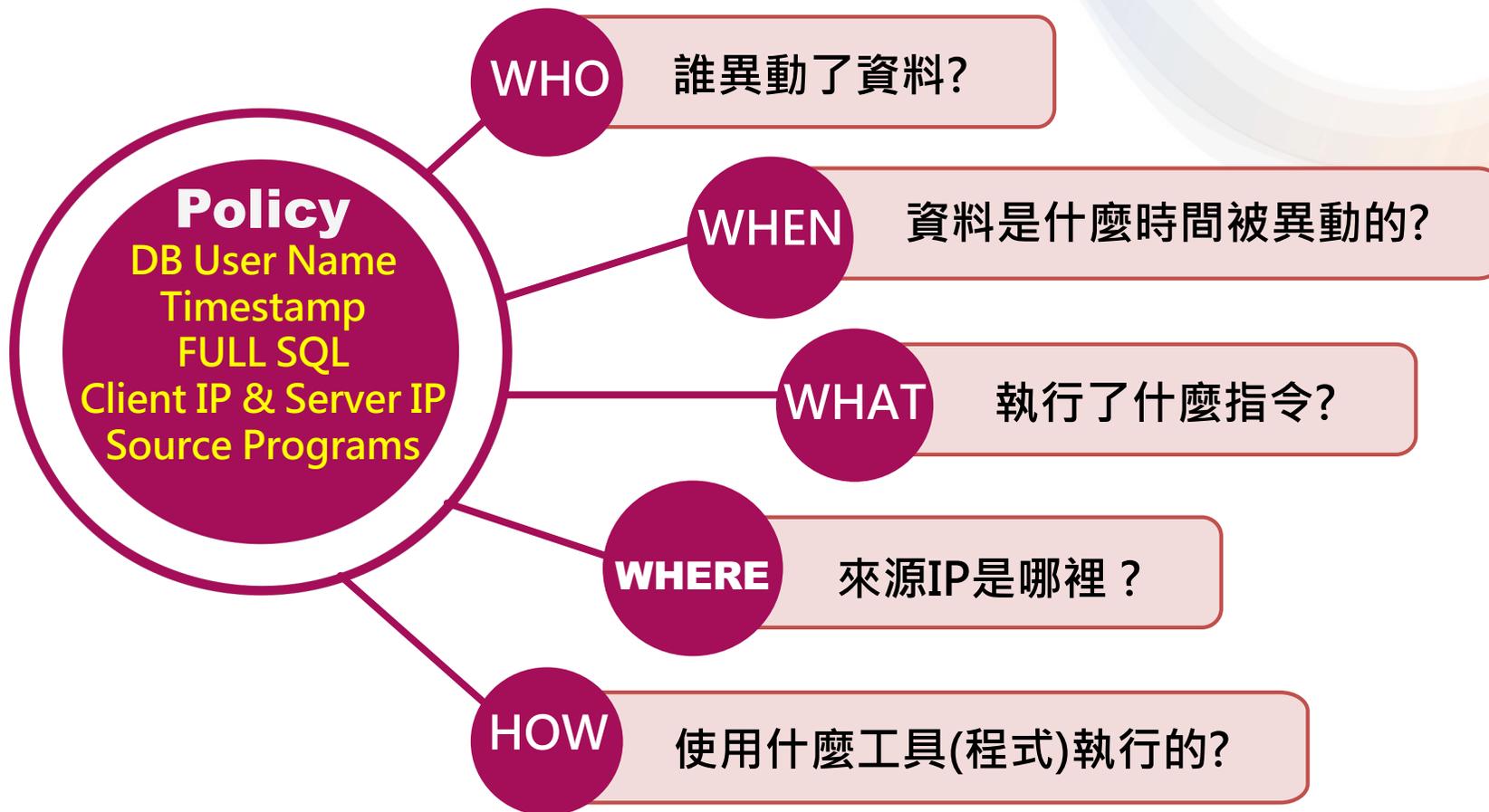
分工監控，重要訊息不遺漏!

設定排程每日寄送報表至相關資訊管理人員信箱提供檢核，大幅的節省管理人員的時間，有效的提昇資安稽核的效率





自訂監控報表可以看到哪些證據?





情境一：學生成績是否被改過？

1

某某老師反應某位學生的成績跟他打的分數不一樣，可以幫我確認是不是有被改過？



教務處同仁

2

請幫我查成績檔這三個月內所有的異動紀錄？



資訊系統負責人

3

我用Guardium查查看唷！



Guardium 管理人

4



不可否認的證據



Guardium 管理者如何自訂監控報表 做為不可否認的證據

1. 自訂 Query Policy

Guardium 管理者登入
Guardium，依資訊系
統負責人的需求設定
Query Policy。

Main Entity: FULL SQL

Add Count Add Distinct Sort by count Partition optimization Run in two stages

Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend	
<input type="checkbox"/>	1	Client/Server	Server IP	Value	<input checked="" type="checkbox"/>	1	<input type="checkbox"/>
<input type="checkbox"/>	2	Client/Server	DB User Name	Value	<input checked="" type="checkbox"/>	2	<input type="checkbox"/>
<input type="checkbox"/>	3	FULL SQL	Timestamp	Value	<input type="checkbox"/>		
<input type="checkbox"/>	4	Client/Server	Client IP	Value	<input type="checkbox"/>		
<input type="checkbox"/>	5	Client/Server	Source Program	Value	<input type="checkbox"/>		
<input type="checkbox"/>	6	FULL SQL	Full Sql	Value	<input type="checkbox"/>		

Query Conditions

AND OR HAVING

Entity	Agg.	Attribute	Operator	Value	Param.
(
WHERE Command	----	SQL Verb	=	Value	update
OR Command	----	SQL Verb	=	Value	delete
)					
(
AND Object	----	Object Name	=	Parameter	table_name1
OR Object	----	Object Name	=	Parameter	table_name2



Guardium 管理者如何自訂監控報表 做為不可否認的證據

2. 輸入查詢條件

輸入條件：2024/6/1起，
異動的「成績檔」

Runtime Parameter Configuration

輸入要查的時間範圍

Enter Period From (QUERY_FROM_DATE)	>=	2024-06-01 00:00:00	→
Enter Period To (QUERY_TO_DATE)	<=	NOW	→

輸入成績檔的
table name

Enter Value for Object Name (table_name2)	=	academic.studscore
Enter Value for Object Name (table_name1)	=	studscore

Show Aliases
(SHOW_ALIASES) On Off Default

Remote Data Source
(REMOTE_SOURCE) -----

Refresh Rate (seconds) 0

OK Cancel



Guardium管理者如何自訂監控報表 做為不可否認的證據

3. 產出報表

Guardium管理者可將報表提供資訊系統負責人判斷是否為正常操作

資料庫IP 執行帳號 執行時間 執行者IP 執行工具 執行的SQL指令

Server IP	DB User Name	Timestamp	Client IP	Source Program	Full Sql
140.1.1.1	FO	2024-06-17 07:50:47	140.1.1.1	D:\SQLSERVER\SQLSERVER\BIDSREPT\SQLSERVER\SQLSERVER.EXE	delete from a where a.rowid in (select a.rowid from s_1 b where a.setyear =b.setyear and a.setterm =b.setterm and a.stud_no =b.stud_no and a.curr_code =b.curr_code and b.setyear =:1 and b.setterm in (:2, :3) and b.score =123)
140.1.1.1	FO	2024-06-17 07:50:50	140.1.1.1	D:\SQLSERVER\SQLSERVER\BIDSREPT\SQLSERVER\SQLSERVER.EXE	delete from a where a.rowid in (select a.rowid from s_1 b where a.setyear =b.setyear and a.setterm =b.setterm and a.stud_no =b.stud_no and a.curr_code =b.curr_code and b.setyear =112 and b.setterm in (2, 3) and b.score =123)



Guardium管理者如何自訂監控報表 做為不可否認的證據

4.提供證據

資訊系統負責人回覆教務處同仁：

是教務處某某同仁的帳號在6/17 7:50用課務管理系統執行兩次刪除。



情境二：學生反應選上的課不見了？

1

某某學生反應他的
某一門課被刪掉了，
但我這裡查不到被
刪除的紀錄？



教務處同仁

2

系統查不到該學生的
課程刪除紀錄，請幫
我查選課檔從這個月
內有沒有某某學號的
刪除紀錄？



資訊系統負責人

3

我用Guardium
查查看唷！



Guardium 管理者

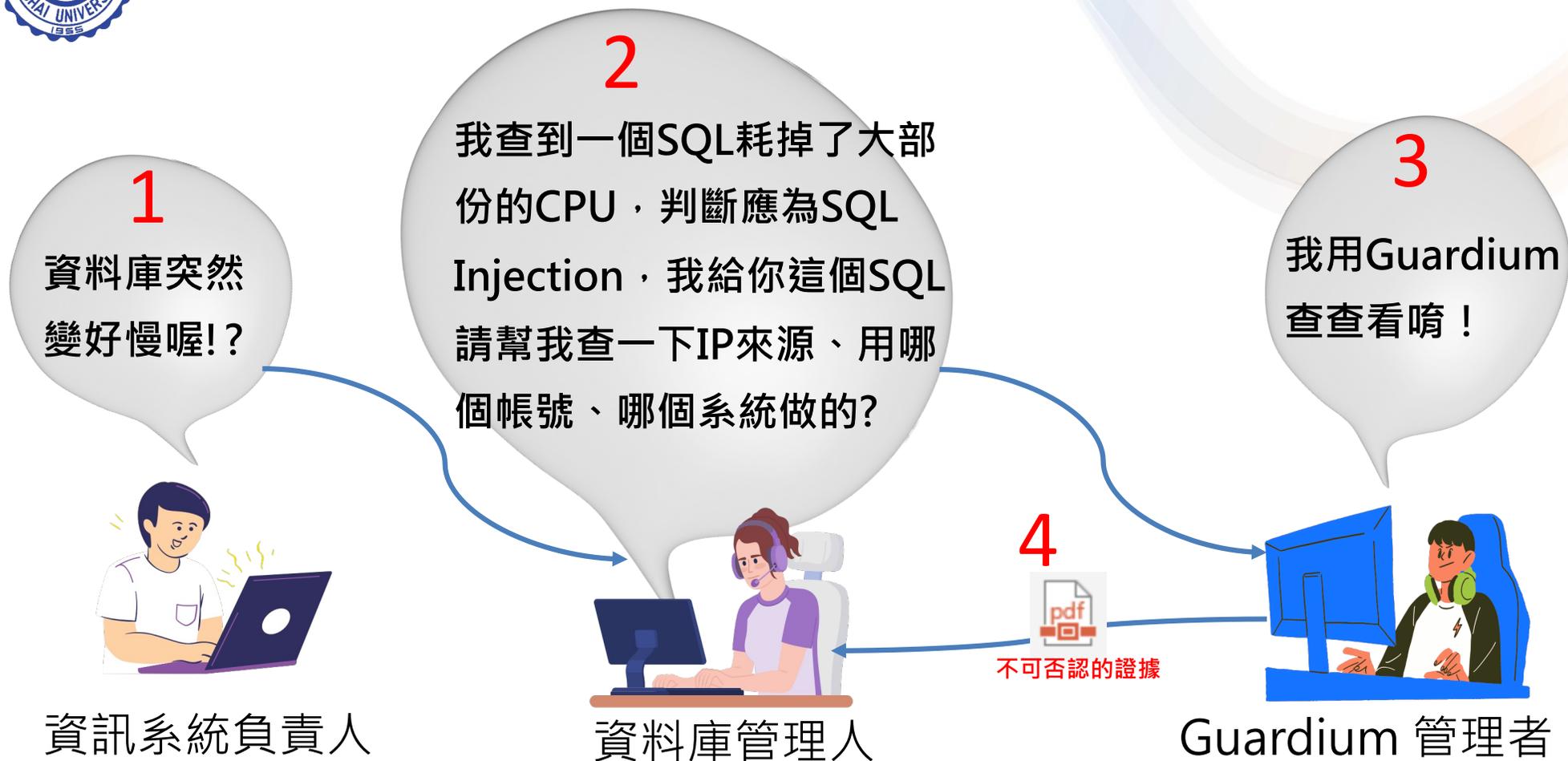
4



不可否認的證據



情境三：提供證據協助資料庫解決問題





情境四：提供每日報表加強監控

1

我發現幾次的SQL Injection駭客常用到 all_xxx這個table，我想每天監控這個table，以及帳號、SQL、使用工具、來源IP。



資料庫管理人

2

我用Guardium建好了，以後每天早上七點都會寄report到你的信箱唷！



Guardium 管理者

3



每日email到DBA信箱的report



情境五：由每日報表發現異常



資訊系統負責人

早上收到的report 傳給你看看，這帳號下的SQL看起來有異，而且使用的是DBEAVER工具，請查查看Web Server是否被駭！



資料庫管理人

All_XXX?
DBEAVER?

Timestamp	Server IP	Client IP	DB User Name	Source Program	Full Sql
2024-07-10 16:56:56	140.128.	140.128.	YOU	DBEAVER 7.2.0 - METADATA	SELECT 'YES' FROM USER_ROLE_PRIVS WHERE GRANTED_ROLE='DBA'
2024-07-10 16:56:56	140.128.	140.128.	YOU	DBEAVER 7.2.0 - METADATA	SELECT U.* FROM ALL_XXX U WHERE (U.USERNAME IS NOT NULL)
2024-07-10 16:56:56	140.128.	140.128.	YOU	DBEAVER 7.2.0 - METADATA	SELECT U.* FROM ALL_XXX U WHERE (U.USERNAME IS NOT NULL)



結論

校務行政資料庫儲存著上百個校務行政資訊系統的重要資料，IBM Security Guardium 除了紀錄資料庫所有的活動行為之外，更是保護資料、加強監控、提供證據最佳利器!



IBM Guardium will help you!

Thank you

