大數據資料檢索

利用elasticsearch 搜索引擎做資安分析

訊達電腦
陳柏霖

目錄

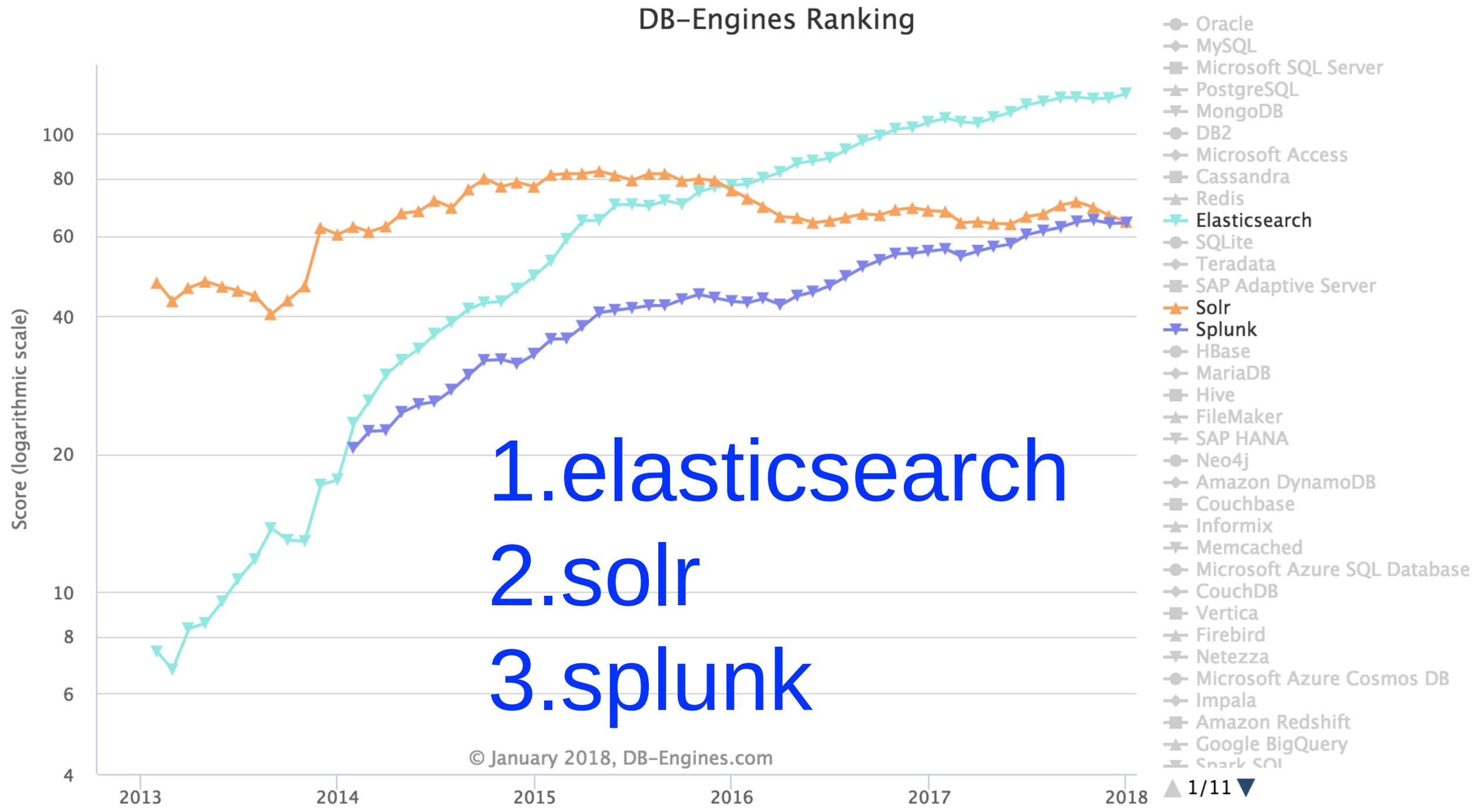
2018年資料庫引擎排名

341 systems in ranking, January 2018

Rank Jan 2018	Rank Dec 2017	Rank Jan 2017	DBMS	Database Model	Score Jan 2018	Score Dec 2017	Score Jan 2017
1.	1.	1.	Oracle	Relational DBMS	1341.94	+0.40	-74.78
2.	2.	2.	MySQL	Relational DBMS	1299.71	-18.36	-66.58
3.	3.	3.	Microsoft SQL Server	Relational DBMS	1148.07	-24.42	-72.89
4.	4.	↑ 5.	PostgreSQL	Relational DBMS	386.18	+0.75	+55.81
5.	5.	↓ 4.	MongoDB	Document store	330.95	+0.18	-0.96
6.	6.	6.	DB2	Relational DBMS	190.28	+0.70	+7.78
7.	7.	↑ 8.	Microsoft Access	Relational DBMS	126.70	+0.82	-0.75
8.	↑ 9.	↓ 7.	Cassandra	Wide column store	123.88	+0.67	-12.57
9.	↓ 8.	9.	Redis	Key-value store	123.14	-0.10	+4.44
10.	10.	↑ 11.	Elasticsearch	Search engine	122.55	+2.77	+16.38
11.	11.	↓ 10.	SQLite	Relational DBMS	114.25	-0.94	+1.88
12.	12.	12.	Teradata	Relational DBMS	72.63	-2.11	-1.54
13.	↑ 14.	13.	SAP Adaptive Server	Relational DBMS	65.46	-0.22	-3.64
14.	↓ 13.	14.	Solr	Search engine	64.37	-1.93	-3.71
15.	15.	↑ 16.	Splunk	Search engine	64.00	+0.21	+8.51
16.	16.	↓ 15.	HBase	Wide column store	61.64	-1.78	+2.50
17.	17.	↑ 20.	MariaDB	Relational DBMS	58.30	+1.56	+13.26
18.	↑ 19.	↑ 19.	Hive	Relational DBMS	55.49	+0.81	+4.35
19.	↓ 18.	↓ 17.	FileMaker	Relational DBMS	55.20	+0.00	+1.72
20.	20.	↓ 18.	SAP HANA	Relational DBMS	46.16	-0.33	-5.77

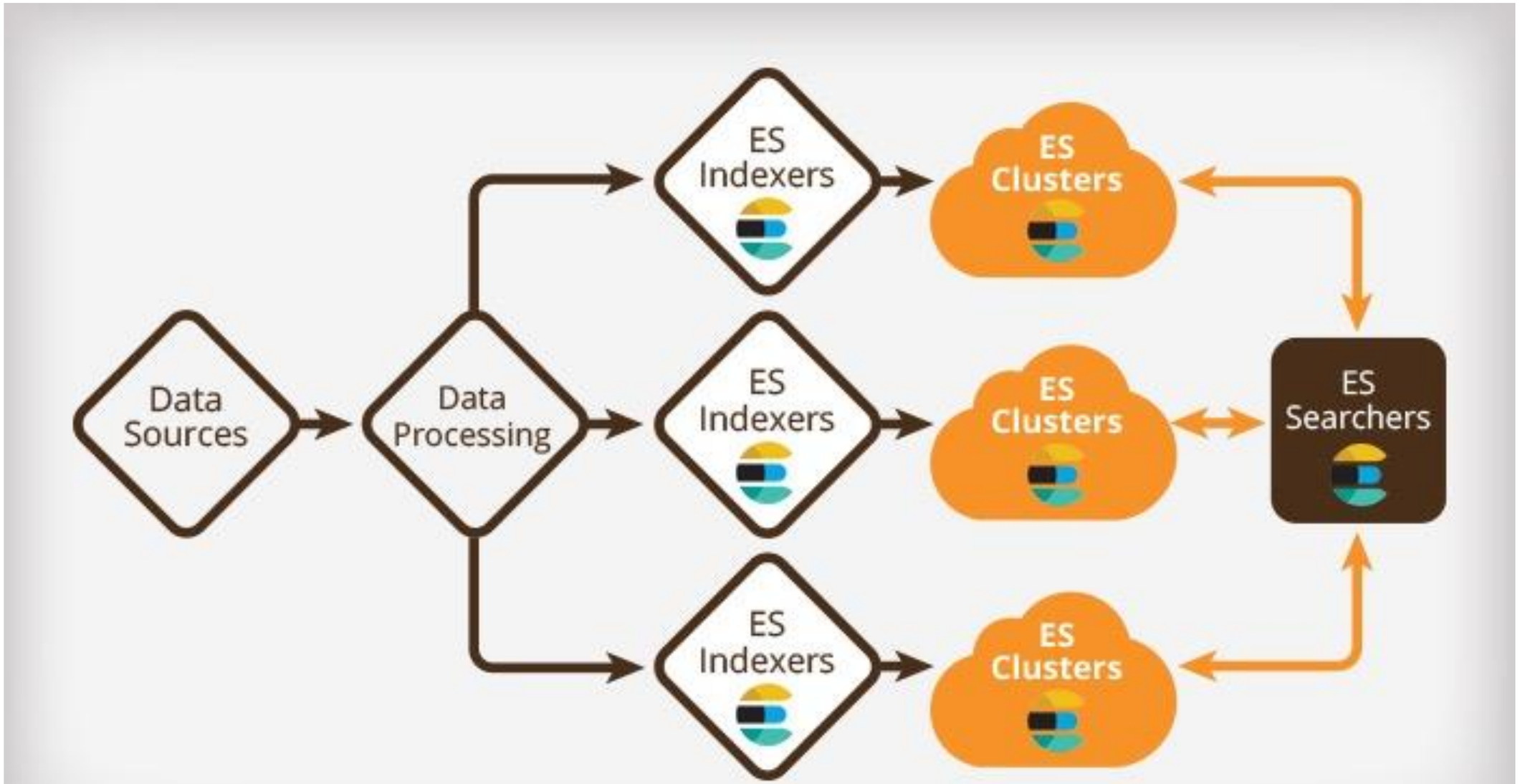
搜索引擎

Top3搜索引擎趨勢分析



大量數據的搜索和分析 – Elasticsearch的應用

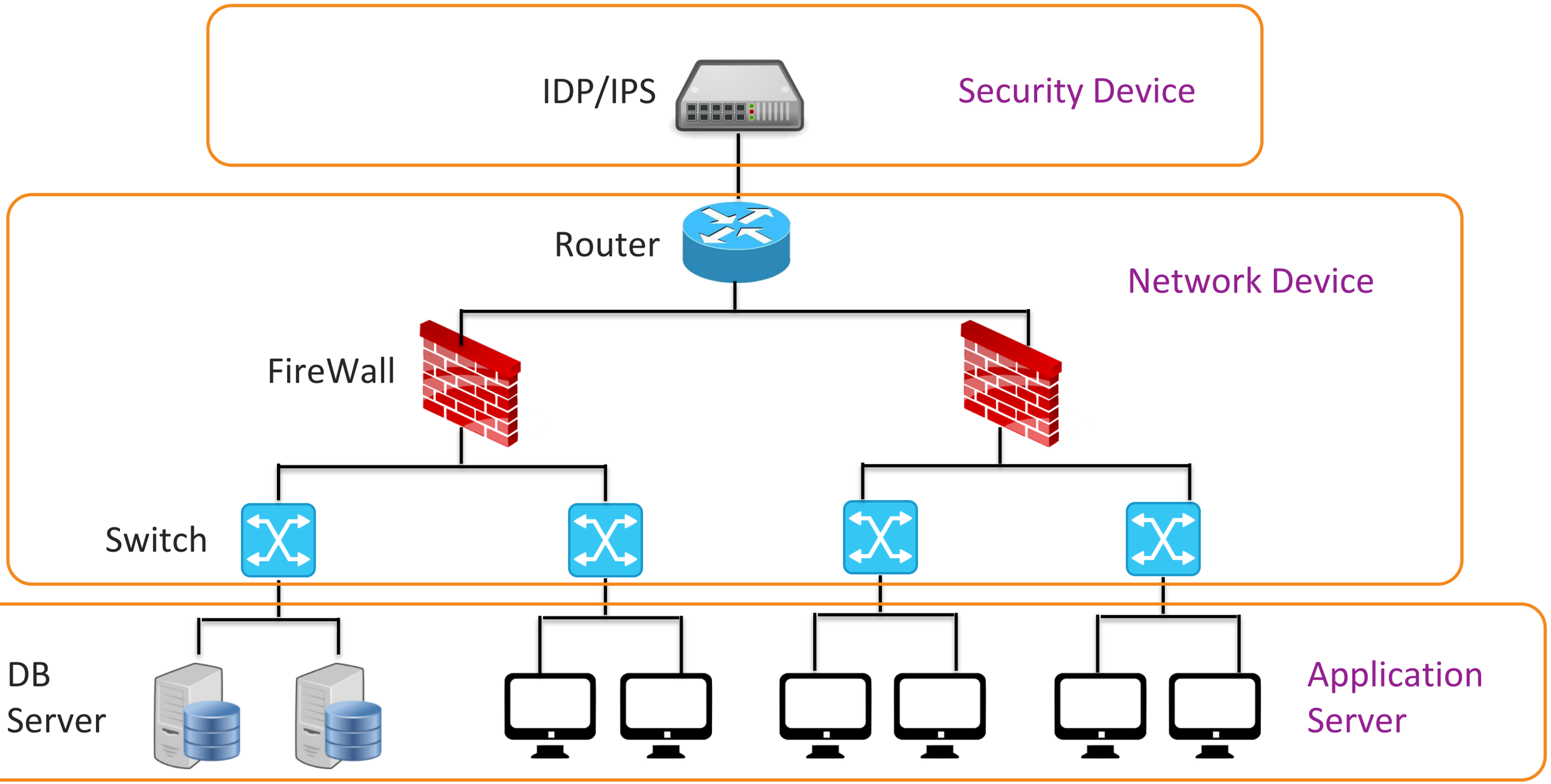
- Elasticsearch
  - 是一個基於 Lucene、支援全文檢索的分散式存儲和**搜索**引擎
  - 主要負責將日誌索引並存儲起來，方便檢索查詢



資安入侵分析

資安入侵檢測的挑戰

- 資安工具眾多，缺乏整合
- **資安**日誌複雜，關聯不易

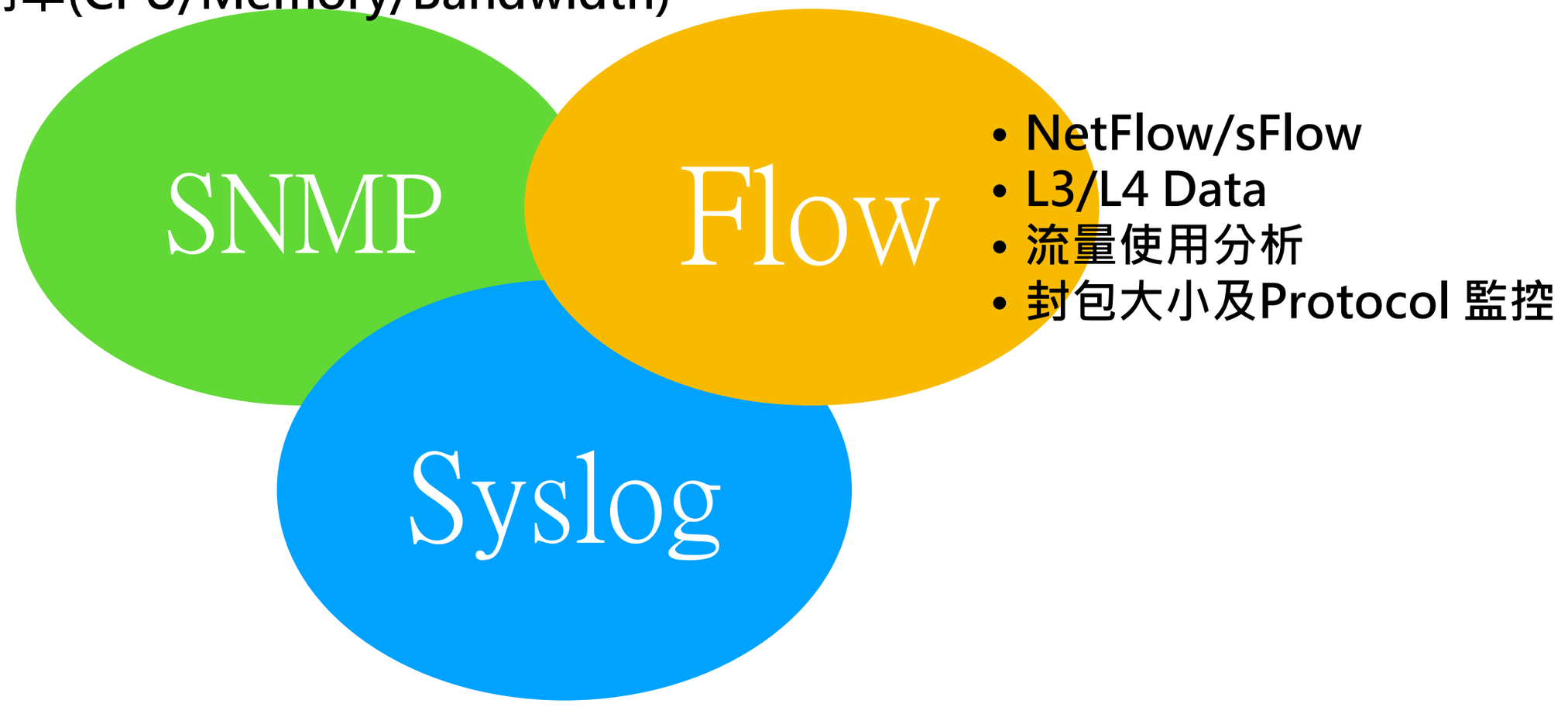


網路大數據的搜索和分析

- 看網路流量
- 查網路異常
- 找網路入侵

網通設備的三種主要協議日誌格式

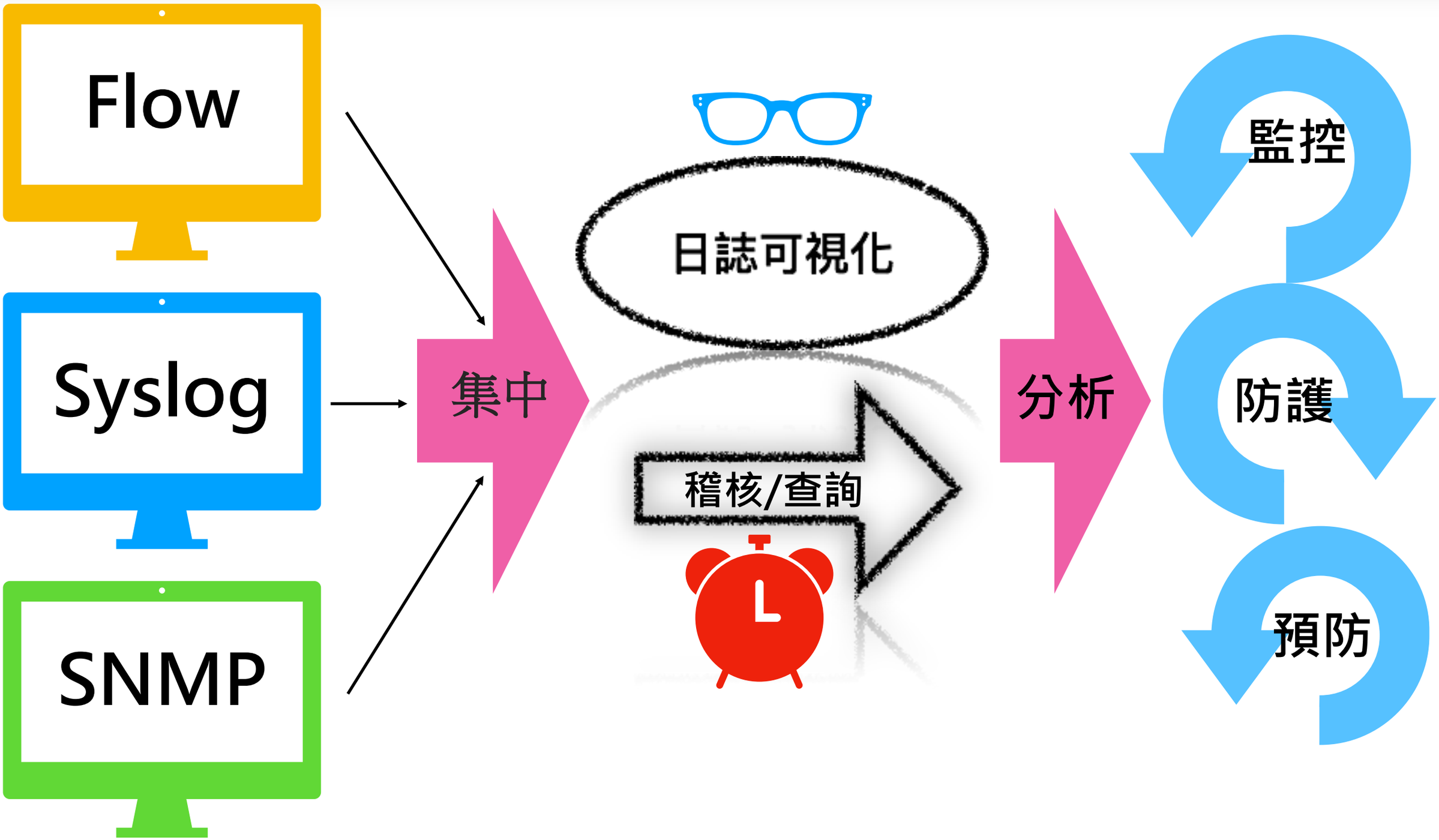
- 設備建健康狀態(Up/Down)
- 效能使用率(CPU/Memory/Bandwidth)



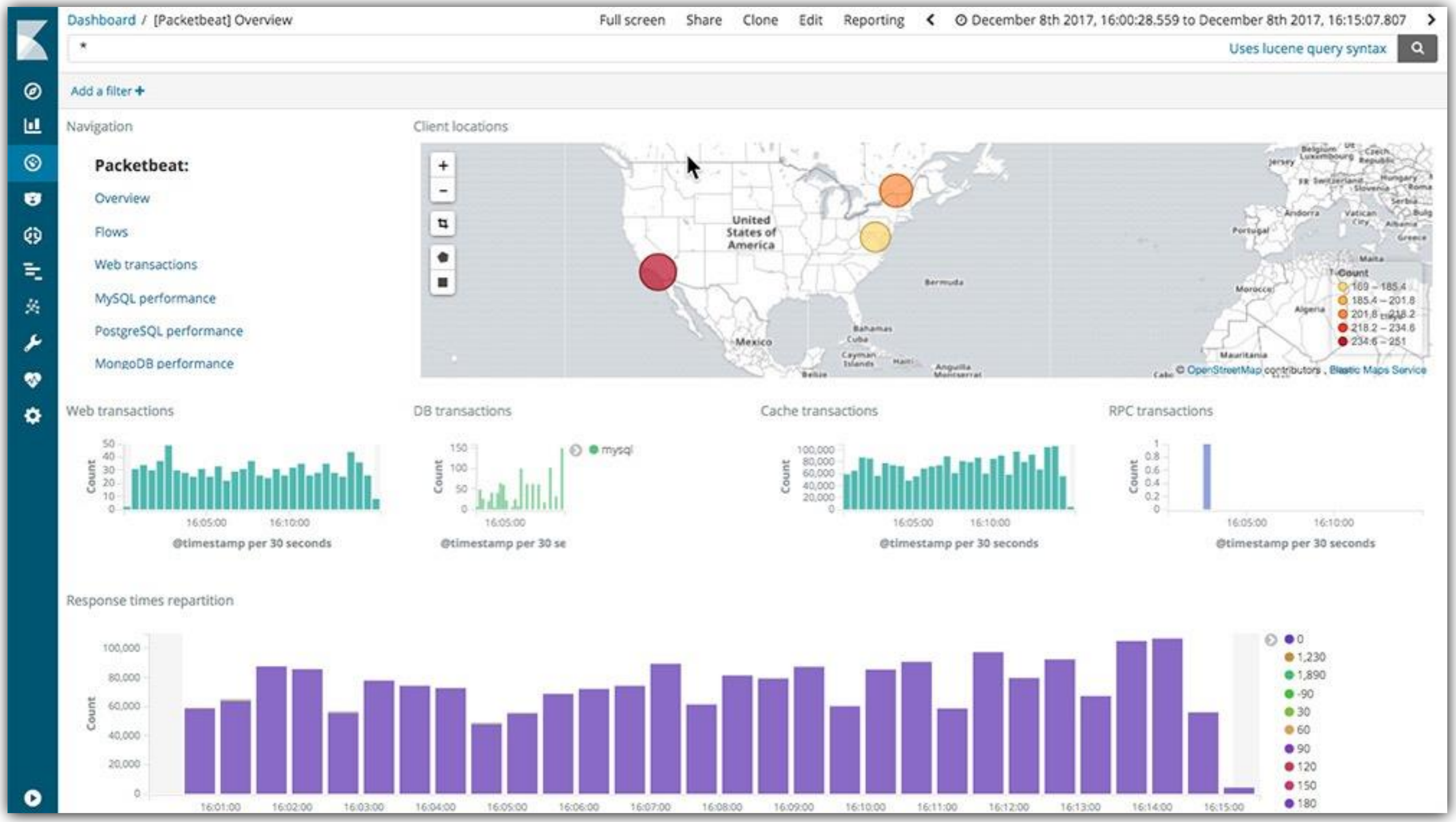
- NetFlow/sFlow
- L3/L4 Data
- 流量使用分析
- 封包大小及Protocol 監控

- 資訊安全，網路設備，伺服器事件關聯分析
- 資安分析應用
- L7 Data

網路管理的進化



更完整的網路搜索分析方案



Windows 系統資安日誌分析

- 整合Windows Server 上的eventlog,做資安入侵的分析

非法login 稽核報警

- 整合Linux Server 上的audit 日誌,做資安稽核的分析

Dashboard / Audit&Secure180-dashboard

Share Clone Edit Last 15 minutes

Search... (e.g. status:200 AND extension:PHP)

Uses lucene query syntax

Add a filter +

audit180-ssh failed

Count

198

Count

audit180-ssh failed detail

addr.keyword: Descending	terminal.keyword: Descending	res.keyword: Descending	Count
58.218.198.167	ssh	failed	112
116.31.116.24	ssh	failed	70
222.187.227.130	ssh	failed	9
178.219.128.186	ssh	failed	7

secure180-ssh Failed password

Count

84

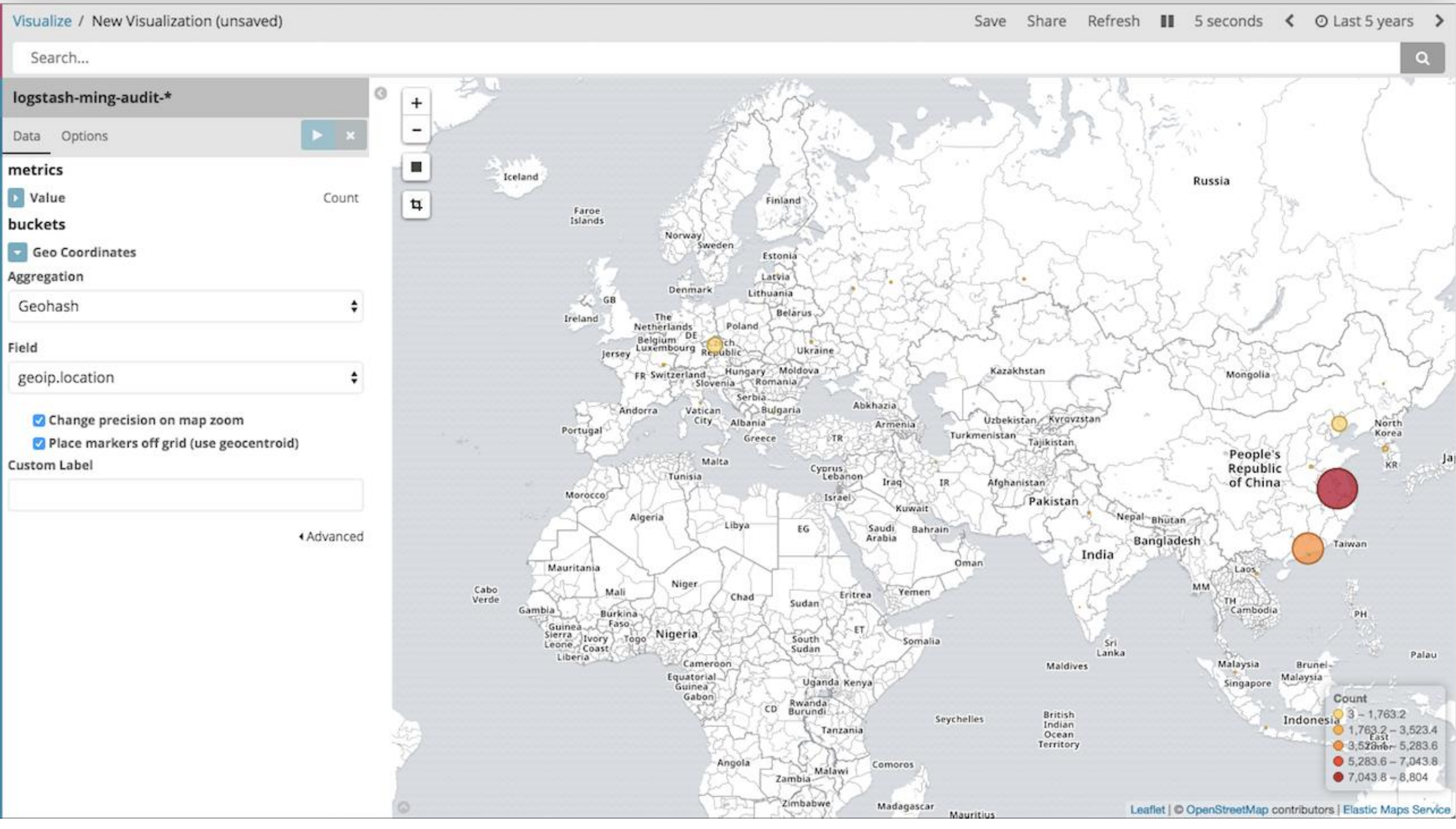
Count

secure180-Detail ssh Failed password

user.keyword: Descending	ip.keyword: Descending	access.keyword: Descending	Count
chris	178.219.128.186	sshd	3
ricardo	222.187.227.130	sshd	3
root	58.218.198.167	sshd	48
root	116.31.116.24	sshd	30

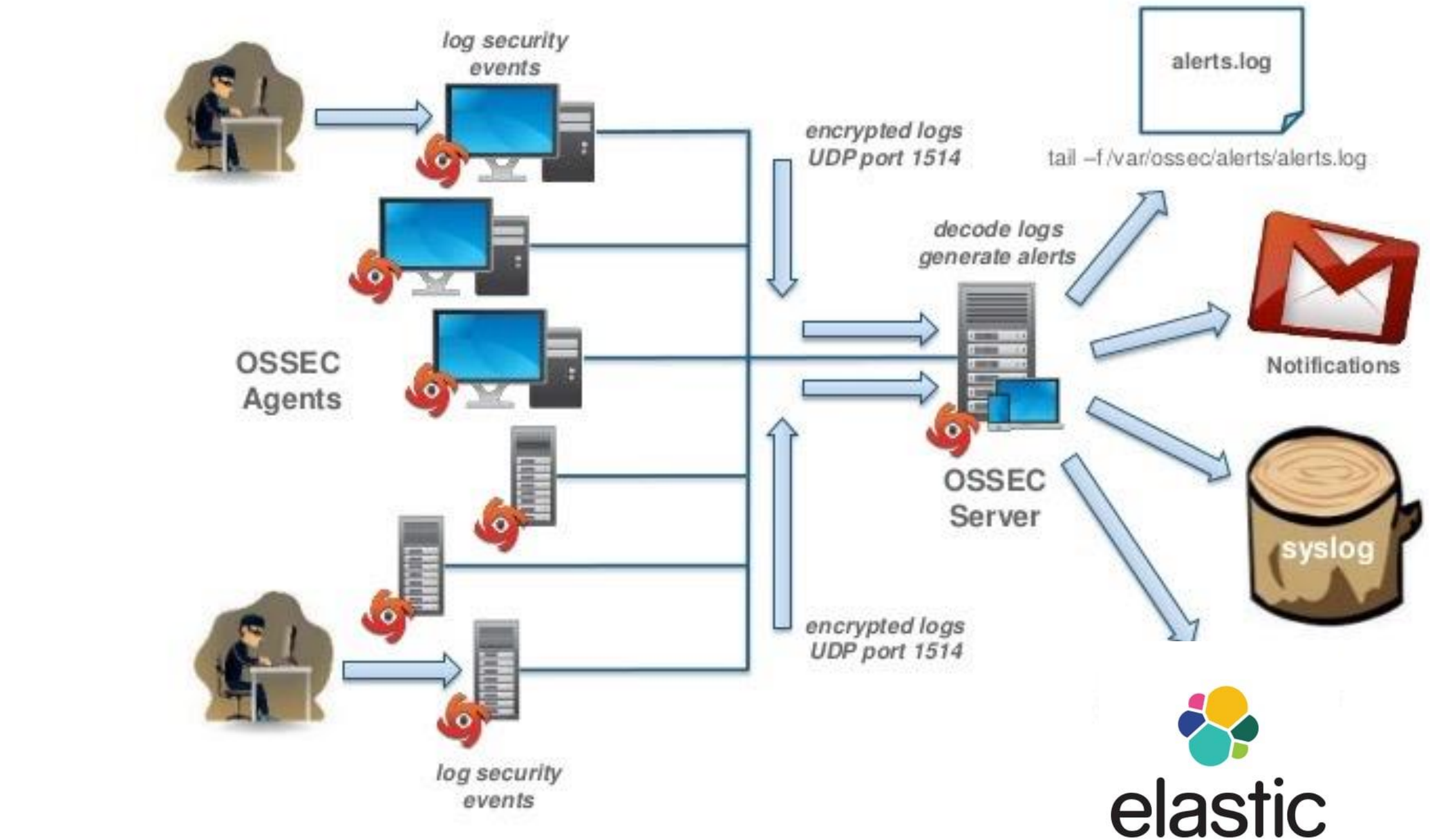
root login 失敗

從資安日誌分析攻擊地點



ES 整合OSSEC 做主機入侵檢測(HIDS)

HIDS是入侵檢測系統，提供主機間的網路數據封包安全管理的監視及分析



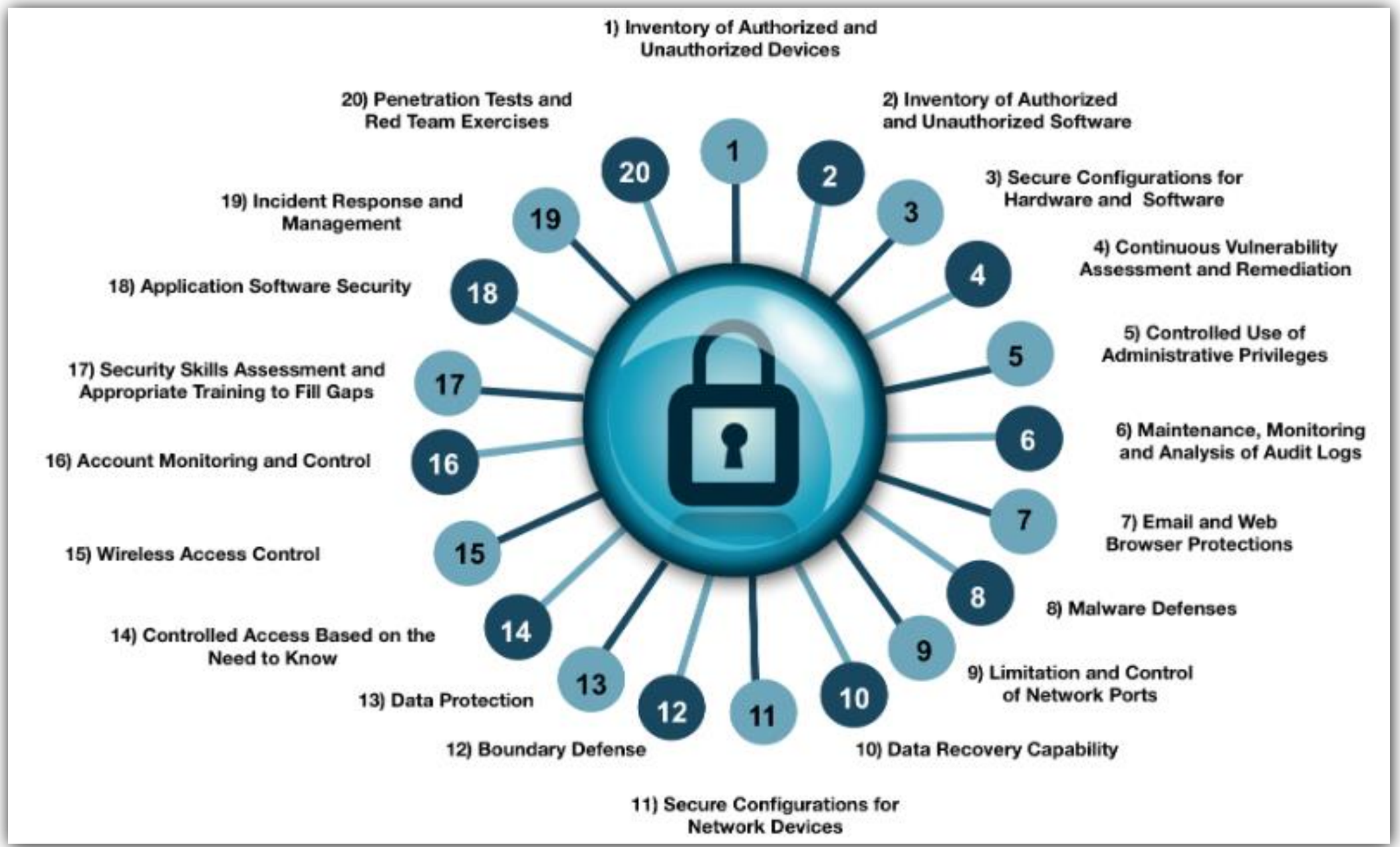
ES 整合OSSEC 做主機入侵檢測(HIDS)

利用ES 系統創建 HIDS是入侵檢測系統的整體分析和告警

資安日誌分析

CIS20 Critical Security Controls 資安參考

國際資安組織 SANS (System Administration, Networking and Security)，發佈
重點資安控制項目指引(CIS, Critical Security Controls)，
用以提供各企業、組織對於資安管理上的參考



CIS20 Critical Security Controls 資安參考

CIS 1: 盤點已授權與未經授權的設備
CIS 2: 盤點已授權與未經授權的軟體
CIS 3: 主機、端點與行動裝置的硬體與軟體的安全設定
CIS 4: 持續弱點檢測與消弭
CIS 5: 針對特權的管理帳號進行控制
CIS 6: 針對稽核紀錄做到維護、監控、分析
CIS 7: 保護 Email 與 Web 瀏覽器
CIS 8: 惡意程式防禦
CIS 9: 針對網路端限制並控制可用的埠號、協定與服務
CIS 10: 資料復原能力
CIS 11: 網路設備的安全設定
CIS 12: 邊界防護
CIS 13: 資料保護
CIS 14: 基於僅需要知道(need-to-know)原則實施存取控制
CIS 15: 無線存取控制
CIS 16: 帳號的監視與控制
CIS 17: 資安職能的評估與訓練
CIS 18: 應用軟體安全
CIS 19: 事件的處理與管理
CIS 20: 滲透測試與事件處理團隊(Red Team)的演練

CIS20 Critical Security Controls 資安參考

CSC 4: 持續弱點檢測與消弭
- 導入自動化的弱點掃描與評估管理工具

CSC 5: 針對特權的管理帳號進行控制
- 針對特權帳號的使用進行追蹤、管制、預防、矯正
- 重要的系統，有需要進行管理權限登入時，可以考慮多因素的強化身分認證，結合智慧卡、憑證、OTP、生物特徵等，避免僅依賴帳號密碼就可以登入操作

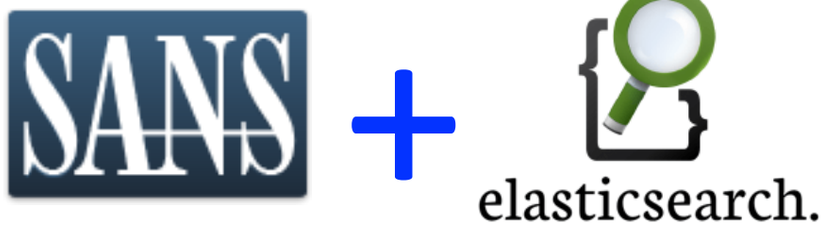
CSC 6: 針對稽核紀錄做到維護、監控、分析
- 所有的系統都要設定開啟正確的稽核紀錄，並且傳送到集中的位置正規化後進行保存與分析
- SIEM的導入

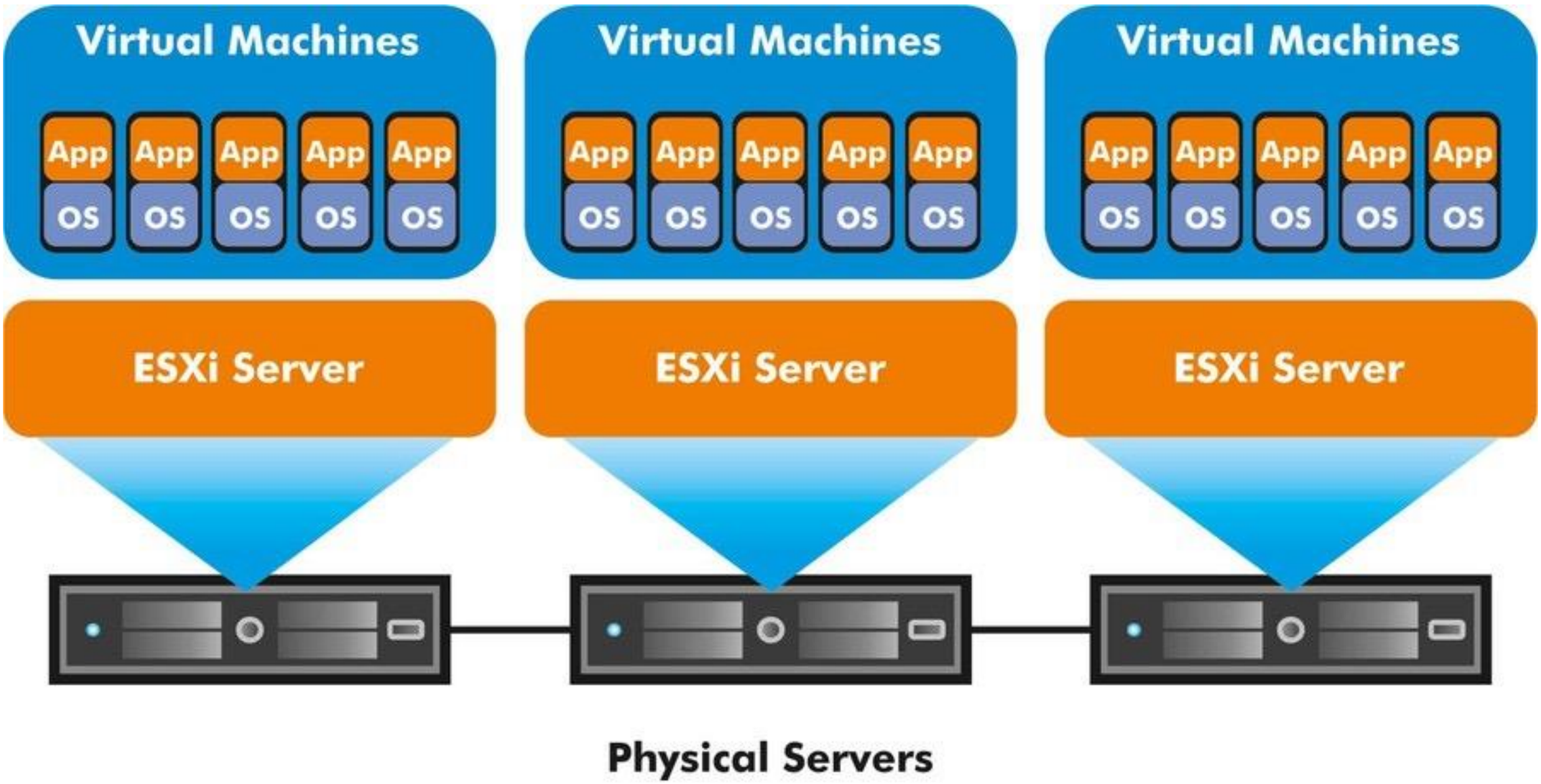
CSC 8: 惡意程式防禦
- 防毒軟體、端點防火牆、Host IPS等機制，以便讓惡意程式無法遁形。
- 建議於網路端，實施非傳統特徵比對方式來過濾惡意程式的下載。
- 建議於DNS端開啟記錄功能，讓查詢已知C2 中繼站的行為得以被記錄，以得知哪個端點已經中了惡意程式後門與木馬

CSC 9: 針對網路端限制並控制可用的埠號、協定與服務

資安稽核分析報告範例

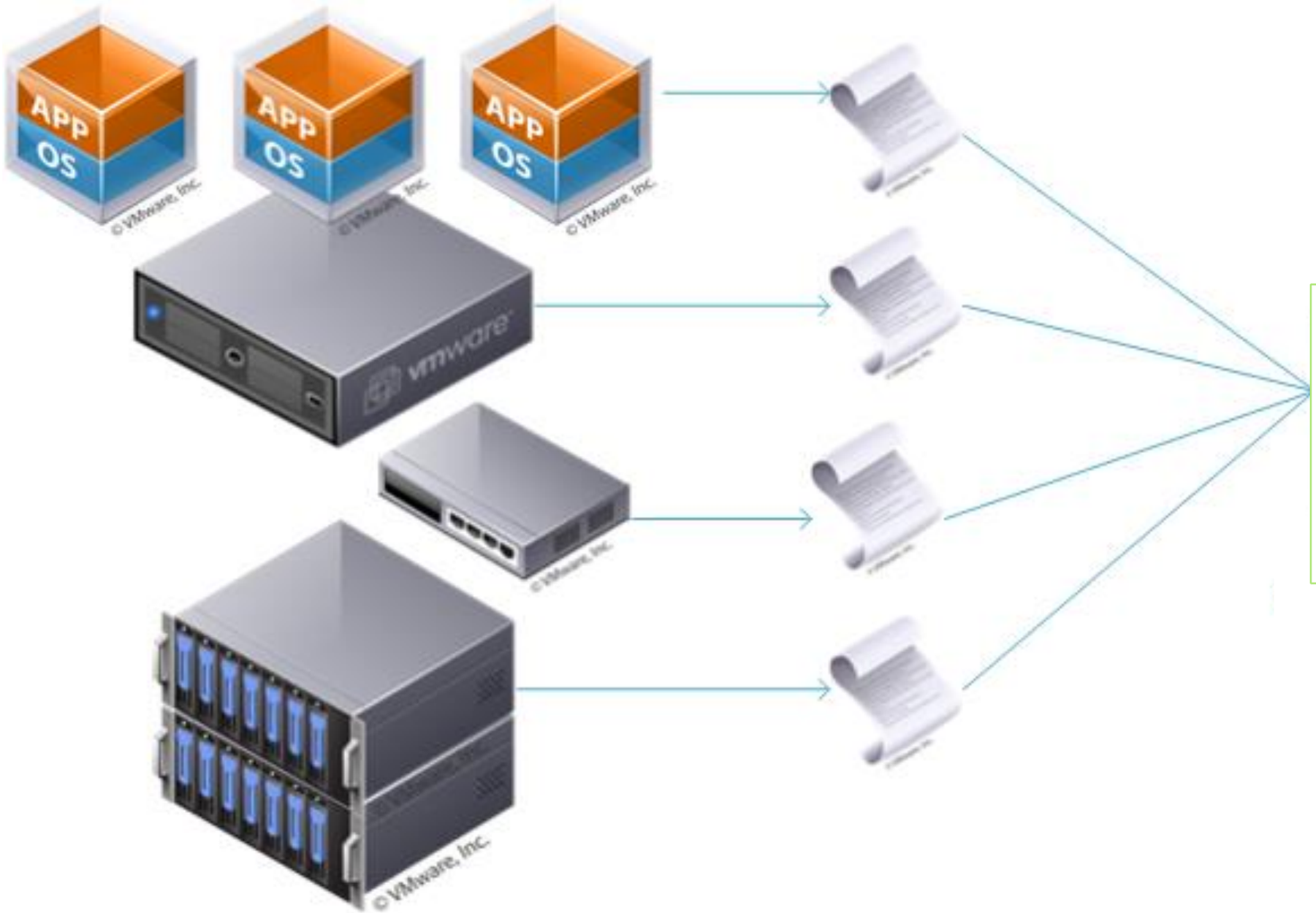
- 收入登入登出log,提供特權帳號詳細報表,並可找出異常登入清單(非上班日登入)
- 收入登入登出log,提供一般帳號登入失敗報表
- 提供各主機系統時間校時報表,確保稽核檔案的時間正確性
- 收入防毒軟體log,提供全體電腦中毒紀錄與病毒碼更新情況,確保各電腦病毒碼為最新
- 收入防火牆log,提供流量報表,即時監控異常流量並告警
- 收入防火牆log,監控特定port進出紀錄
- 收入防火牆log,提供內部人員異常
- 收入資料庫稽核log,提供特權帳號存取紀錄
- 收入資料庫log,提供敏感資料表存取紀錄
- 收入資料庫log,提供危險指令存取紀錄
- 收入盤點軟體的log,提供未經授權的電腦報表,即時監控異常連線並告警
- 收入組態管理工具的log或直接監控目錄,提供重要檔案異動報表
- 收入弱點掃描工具的log,提供已知弱點報表
- 收入備份軟體log,提供各排程執行紀錄,確保日常備份正常運行
- 收入無線controller連線log,提供各電腦連線紀錄,找出異常連線清單
- 提供各主機連線情況報表,確保網路正常
- 整合以上各種軟體log,提供各電腦的全方位資訊,為各主機負責人整合性儀表板,減少發現問題/解決問題的時間



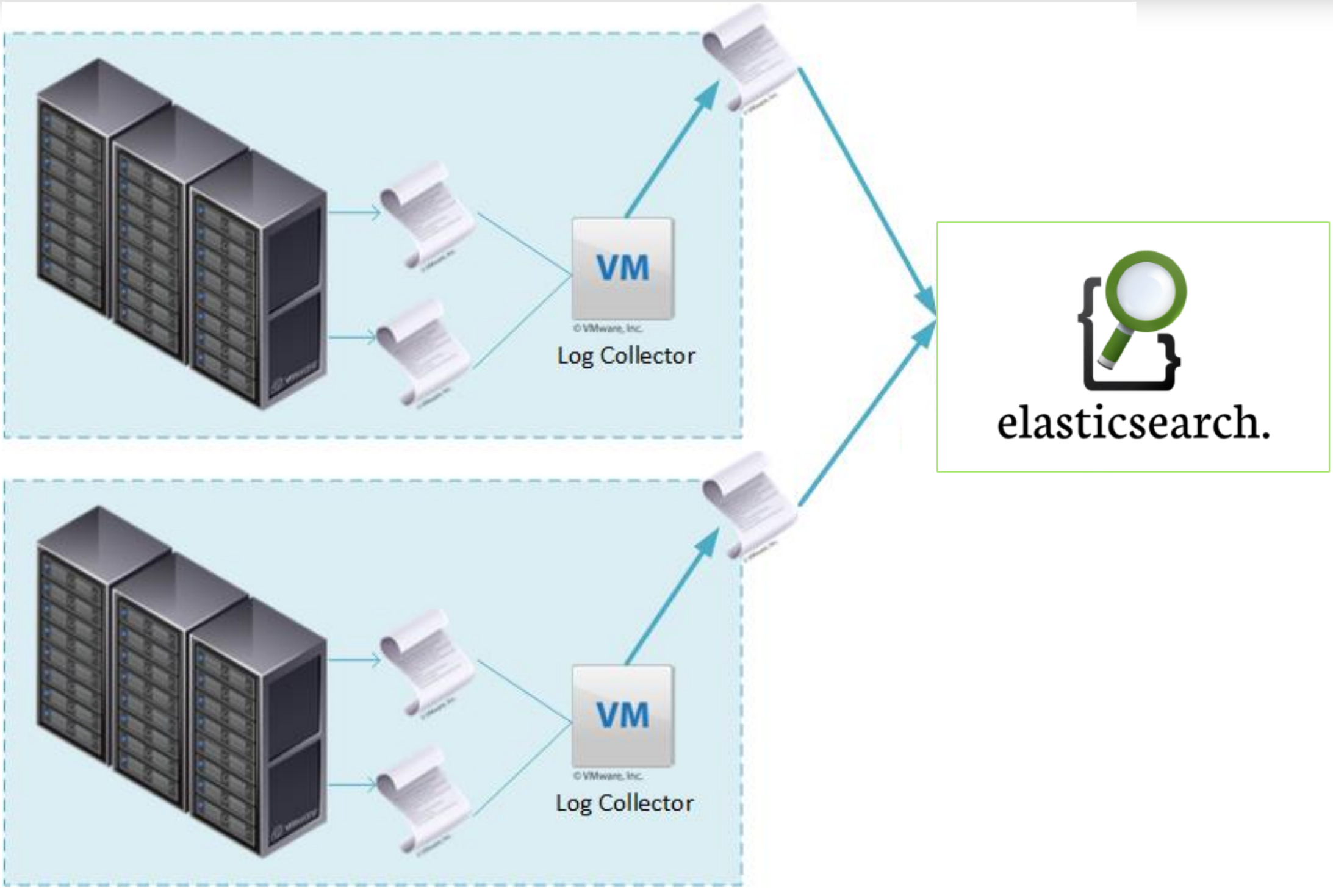

Virtual Machines
App
OS
Virtual Machines
App
OS
Virtual Machines
App
OS
ESXi Server
ESXi Server
ESXi Server
Physical Servers

VM 管理應用

VM 日誌收集搜索分析

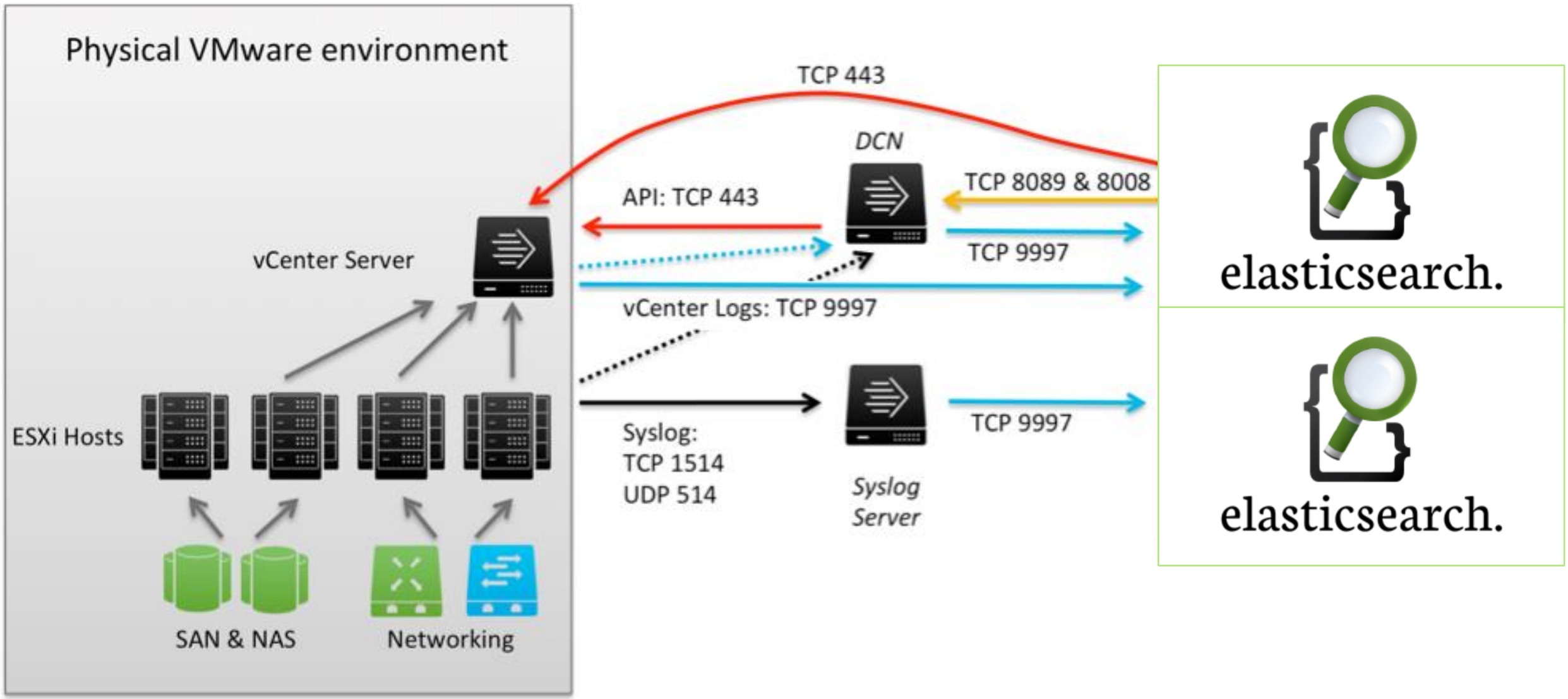

APP
OS
APP
OS
APP
OS
© VMware, Inc.
vmware
© VMware, Inc.
© VMware, Inc.
© VMware, Inc.
elasticsearch.

VM 日誌收集搜索分析


VM
© VMware, Inc.
Log Collector
VM
© VMware, Inc.
Log Collector
elasticsearch.

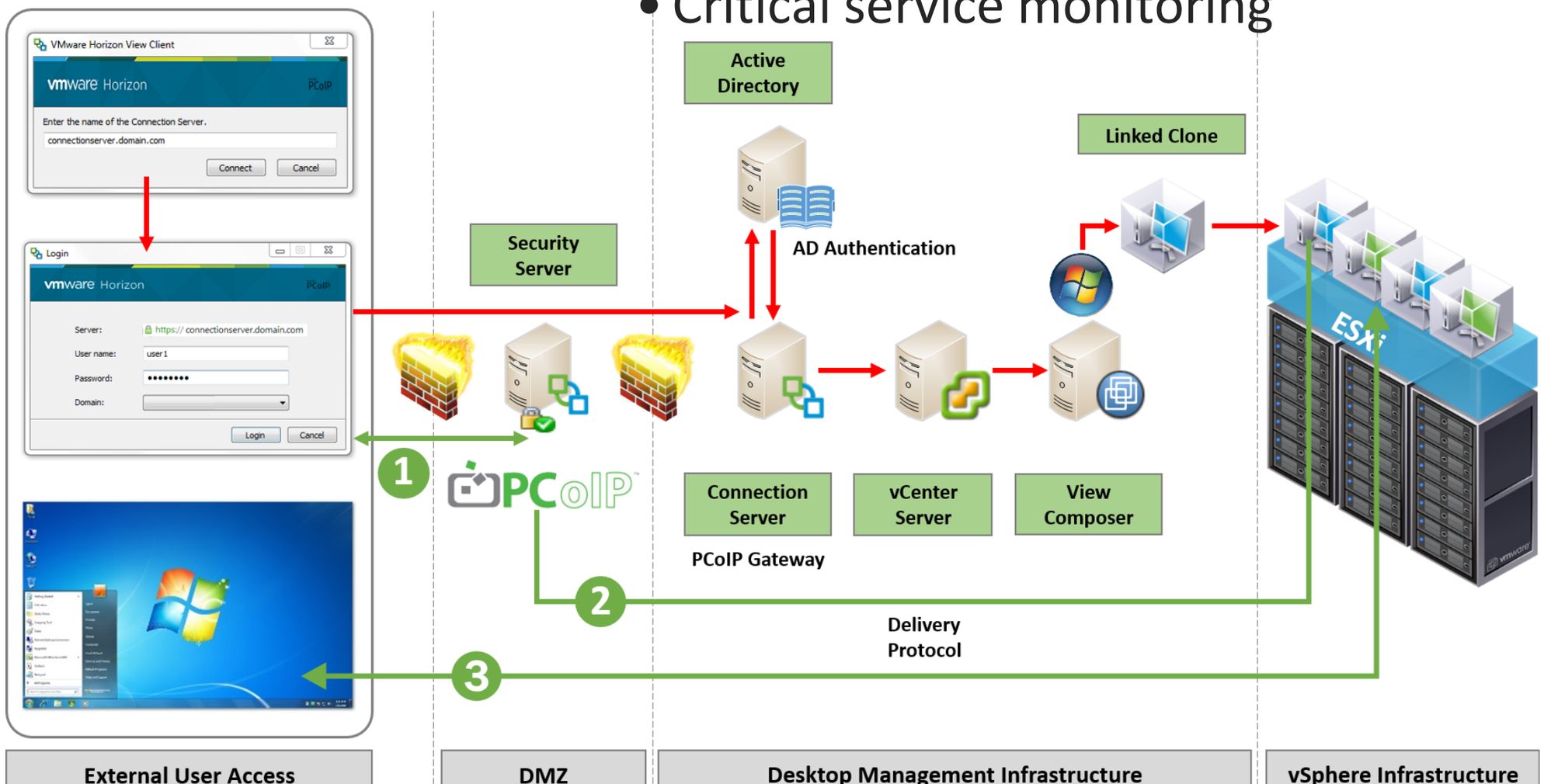
VM 日誌搜索分析內容

- vCenter logs
- ESXi logs
- Performance Metrics



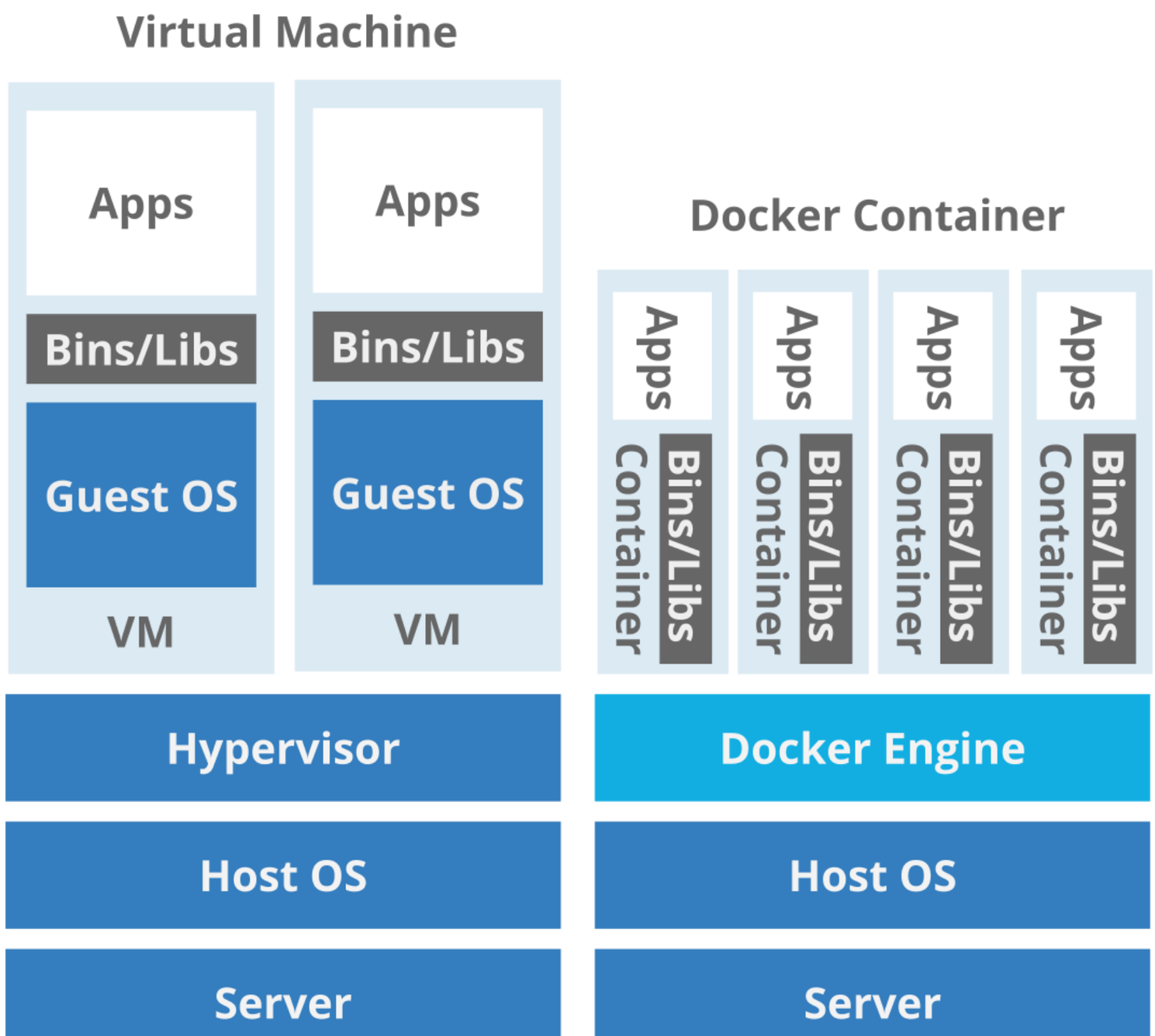
VDI 日誌搜索分析

- ICA latency reporting
- User experience investigation
- User logon time details
- Performance visualization and monitoring
- Application usage
- Critical service monitoring



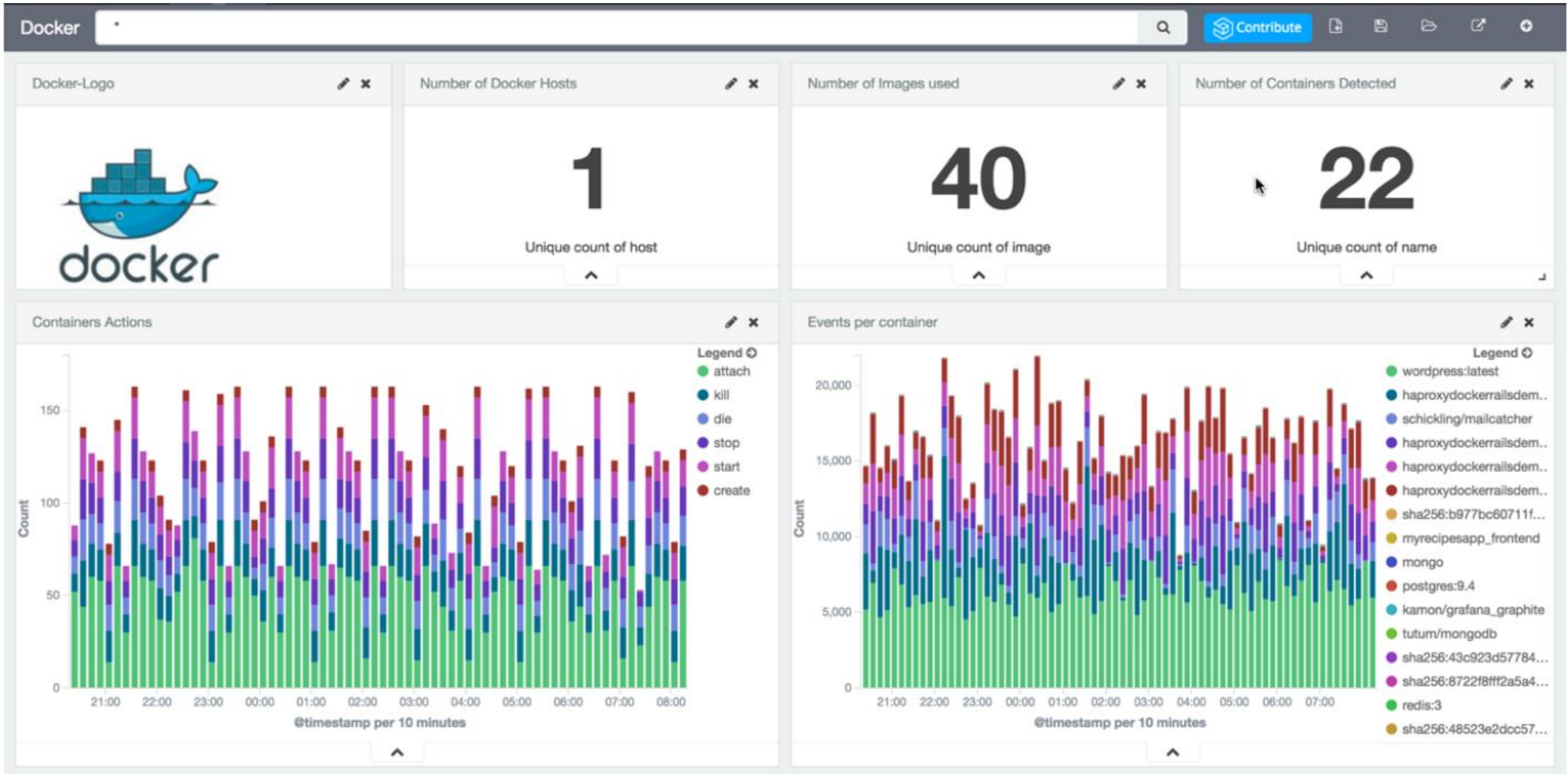
ES 在Docker 管理應用

利用elasticsearch 管理docker



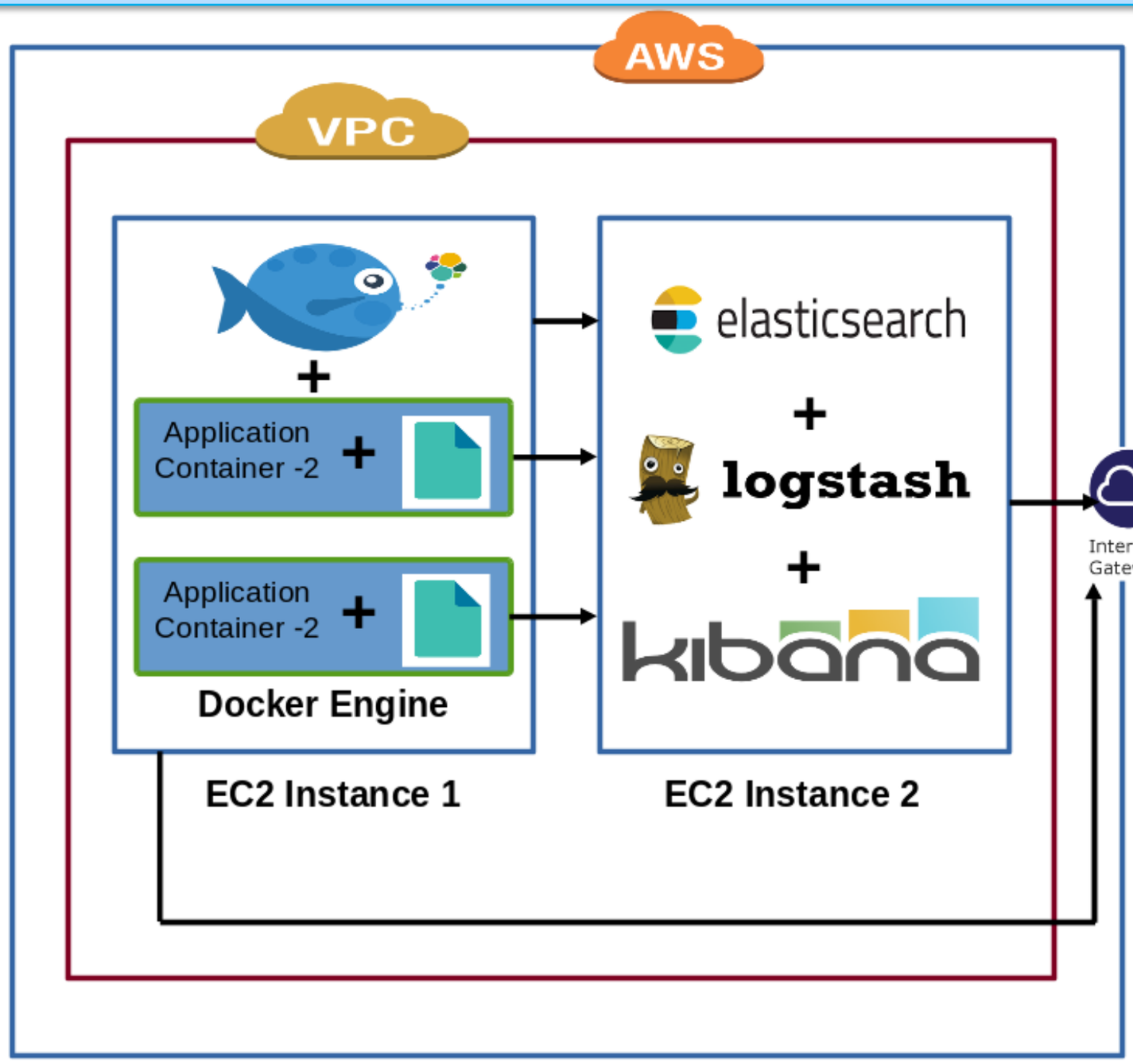
利用elasticsearch 管理docker

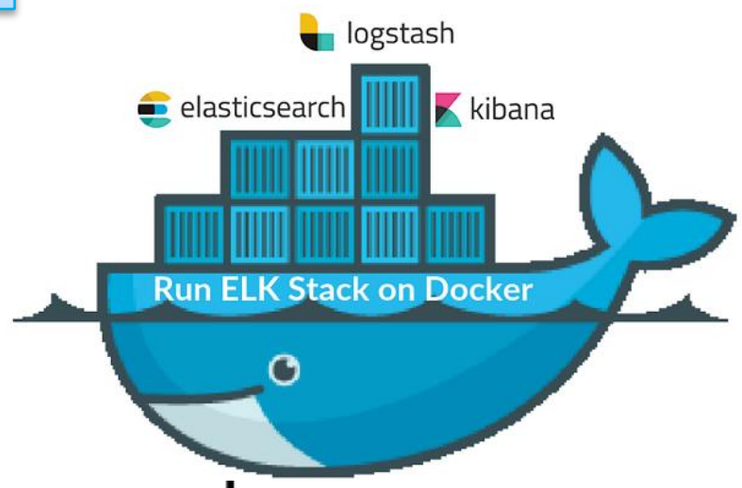
將ES 部署在docker 上， 並且管理docker 的資源



使用ES 管理Docker 的系統結構

將ES 部署在docker 上， 並且管理docker 的資源





Business User

大數據資料檢索

利用elasticsearch 搜索引擎做資安分析

訊達電腦