ManageEngine

Log360

全方位 SIEM & AD
日誌與資安事件分析管理系統

bluechip infotech

Helping your business grow

藍籌科技
張慶振
Kerry Chang

11 JAN 2021 NEWS

Over 100,000 UN Employee Records Accessed by Researchers

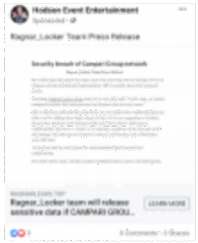
一群資安研究人員，發現聯合國曝露了一些Git憑證，進一步得以下載該Git儲存庫，並發現**大量的聯合國員工個資**，估計有超過10萬筆員工個資外洩...

最終，研究人員直接通報聯合國。

但並非所有單位都這麼幸運

挾持資訊進而勒索已成趨勢

- 在這種有利可圖的情況，類似攻擊只會有增無減



新聞

【2021資安大預測】趨勢4：勒索軟體攻擊｜讓受害者難堪成勒索的目標

駭客揚言將資料外洩做為要錢手段已是2020年的常態，但在此同時，也有攻擊者開始採用更激烈的方式，脅迫受害者付贖金

文 / 周峻佑 | 2021–01–11

新聞

【2020十大資安趨勢1：資料外洩】管理不周導致資料外流事件頻傳，企業、雲端業者、政府均應強化管理

2019年的資料外洩事件，有不少是發生在外部廠商，或者是已經下線的系統，徹底盤點和控管，成為企業資安需要加強的面向

文 / 周峻佑 | 2020–01–09

沒有人是局外人

- 號稱「史上最嚴格個資法」的一般資料保護規定（General Data Protection Regulation，簡稱GDPR)
- 法規的基礎，是「被遺忘權（right to be forgotten）」
- GDPR準則：
  - 需執行個資保護風險評估
  - 需任命資料保護長
  - 具備即時通報
  - 禁止向第三國傳輸個資。

保護個資，至關重要

- 任何地方都有可能遭受攻擊
  - 外部威脅
    - 網路/資安設備
    - 雲端平台服務
  - 內部威脅
    - Active Directory
    - 應用程式/資料庫
    - 伺服器/終端裝置

Log360能幫助您什麼？

What can Log360 do for you?

整合式方案，內部外部一網打盡

ADAudit Plus
即時 Active Directory
變更稽核解決方案

EventLog Analyzer
協助您日誌管理
/分析/報表產出

Exchange Reporter Plus
協助您管理本地與線上
Exchange之報表產出/
稽核與監控

O365 Manager Plus
協助您管理
Microsoft 365報表
/稽核與告警

Cloud Security Plus
整合式公有雲平台
日誌收集監控與報
表產出解決方案

情報收集，搶得先機

1. 日誌管理
   - 支援超過750多種日誌來源
   - 彙整、分析、鑑識
2. 即時事故管理
   - 特權存取稽核
   - 偵測、回應、告警
3. 威脅情資整合(Threat intelligence)
4. 使用者和實體行為分析(UEBA)
5. IT合規管理

Log360幫助您 – 預防篇 (Security Event)

- 監控所有網路活動，解決IT營運問題，確保網路安全
- 及早識別威脅，防止資料外洩
- 偵測不尋常的使用者行為，感知攻擊，快速因應
- 協助企業遵守IT法規

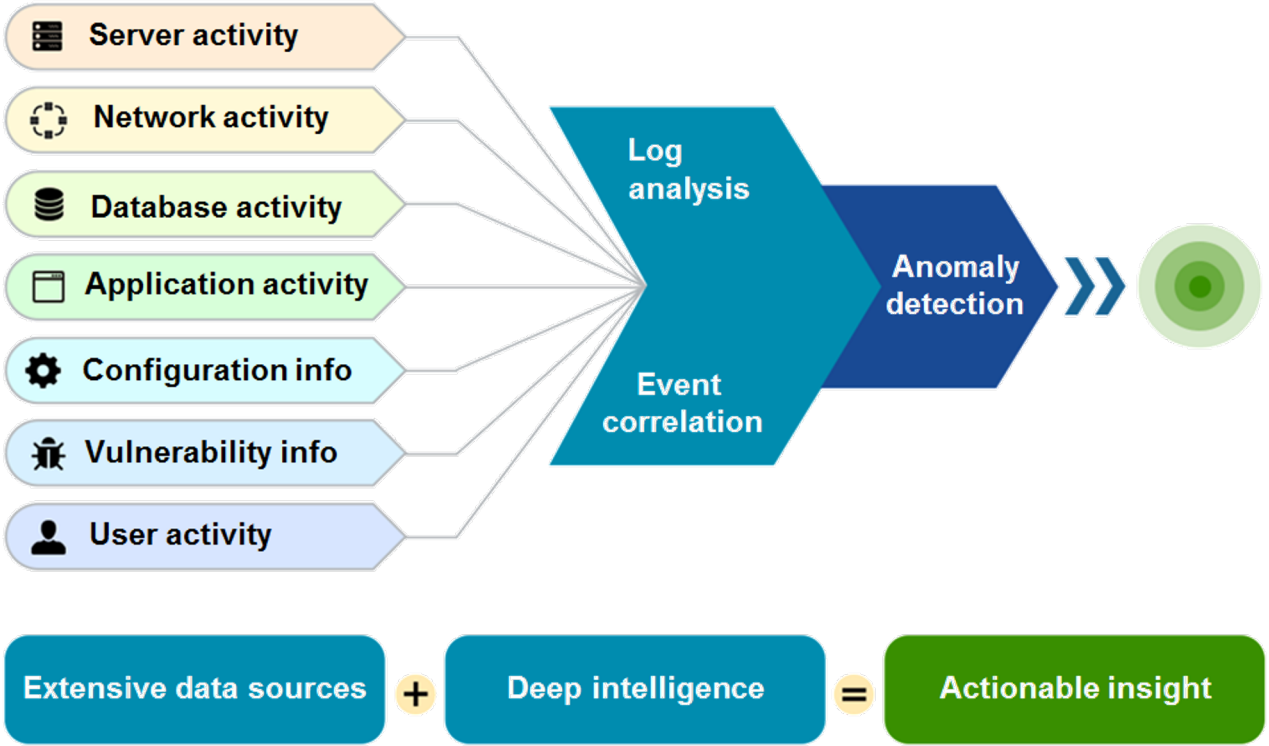
輸入密碼錯誤，一分鐘超過240次

240次嘗試登入後，登入成功

Log360幫助您 - 治療篇 (Security incident)

- 針對每件資安事故發出即時告警，管理者優先處理威脅
- 不幸發生事故，也可以提供鑑識分析，及早恢復營運。

海納百川，去蕪存菁

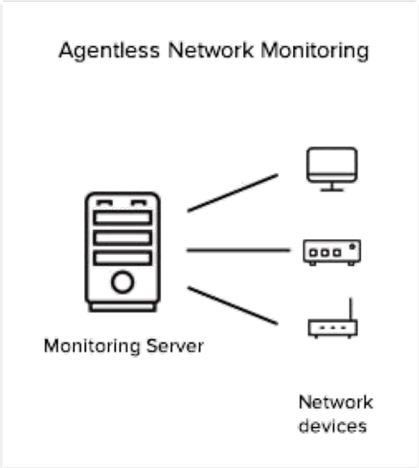

Server activity
Network activity
Database activity
Application activity
Configuration info
Vulnerability info
User activity
Log analysis
Event correlation
Anomaly detection
Extensive data sources
+
Deep intelligence
=
Actionable insight

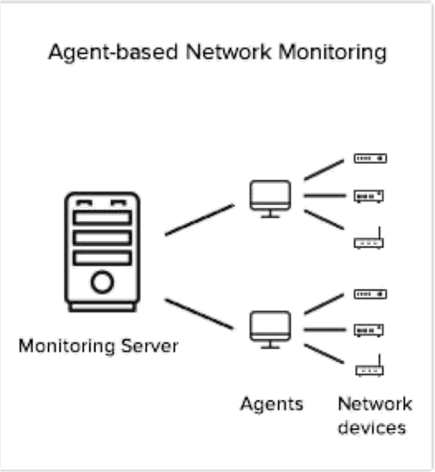
日誌管理

Log Management

日誌收集 - 支援超過750種日誌來源

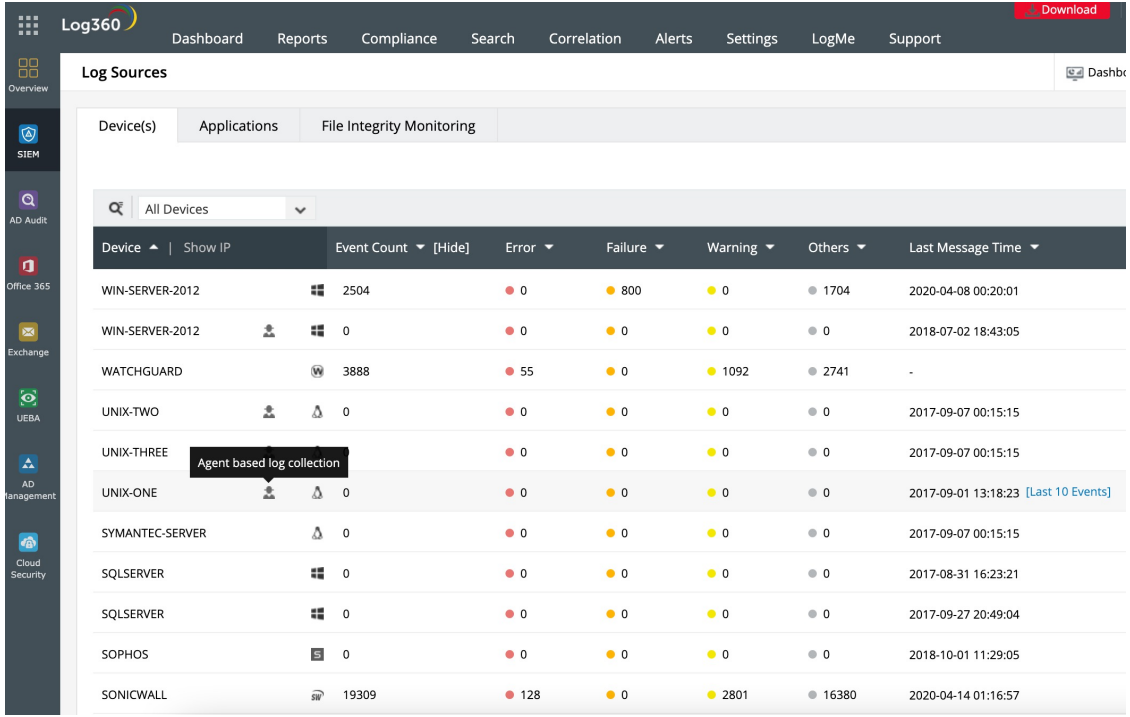
- 支援有Agent/無Agent/API 3種模式：
  - Agentless (大部分情境/網路設備無法安裝Agent)
  - Agent-based (外點/限制區域/DMZ等)
  - API (雲端/虛擬化)





日誌收集 - 範例

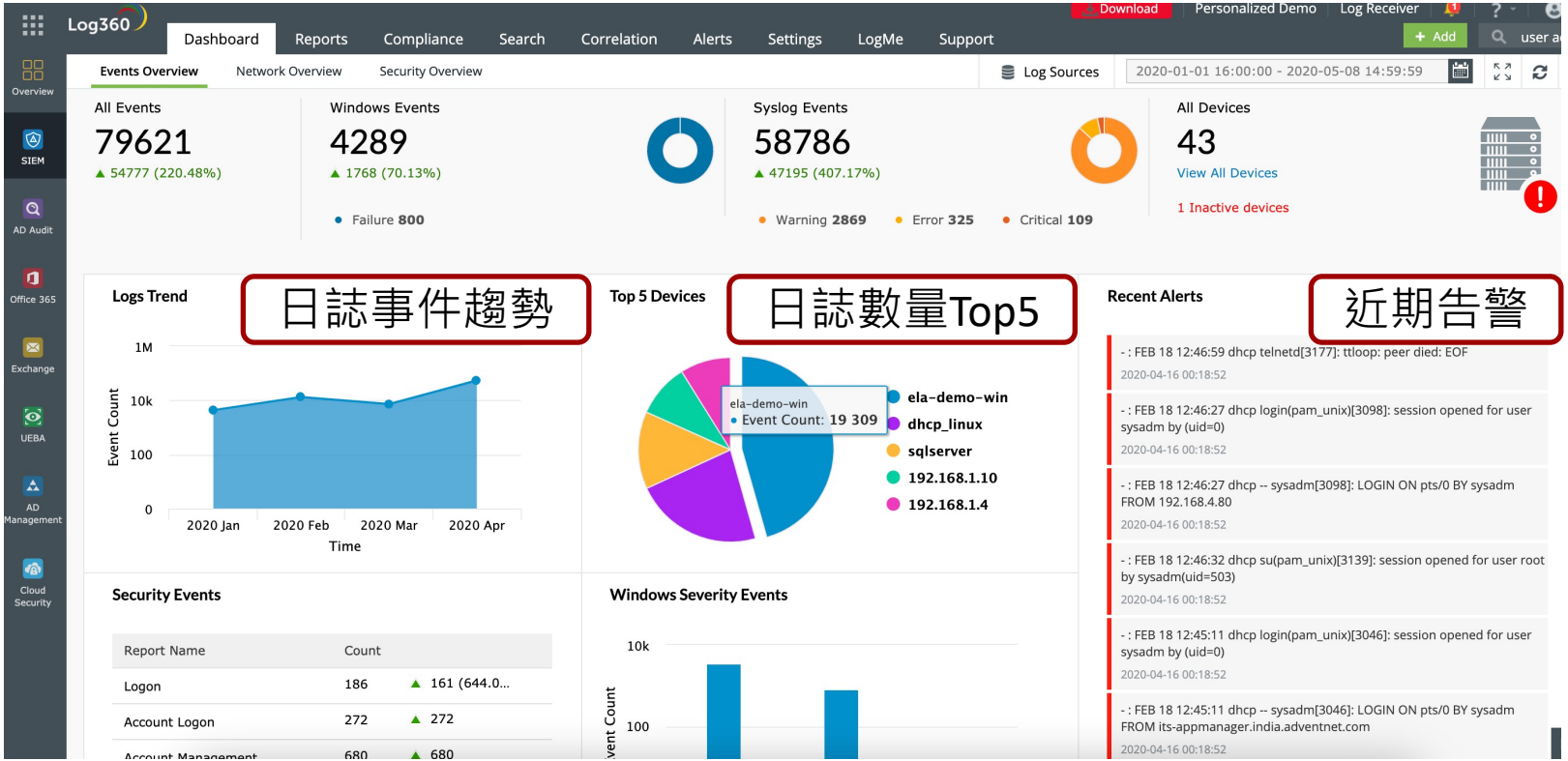
- 支援各式設備
- 即時掌握現狀



日誌分析 - 易讀的資料視覺化

- 上千種報表與告警範本，滿足您資安、稽核、合規的需求
- 也可以自訂報表與告警，滿足特定需求
- 透過快速，易用的強大搜索引擎，深入執行日誌解析並搜尋數百萬條日誌，該引擎可以處理：
  - 每秒20,000筆syslogs
  - 每秒2,000筆 Windows 事件日誌

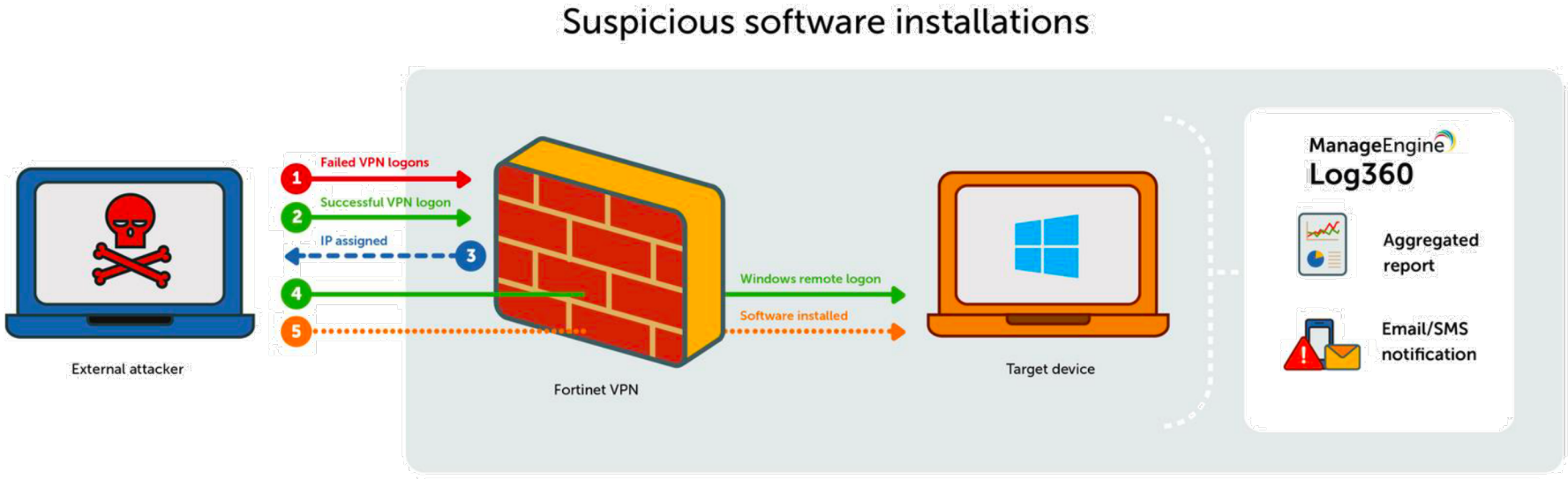
日誌分析 - 範例 - 可自訂儀表板



日誌分析 - 關聯性分析

- 透過30多種預設關聯性規則，在多種設備上偵測攻擊模式
- 偵測像是可疑軟體安裝，或者是蠕蟲等其他網路攻擊
- 以時間軸的方式呈現，匯總日誌軌跡
- 客製化製作關聯性規則，因應不同營運環境的攻擊偵測

一連串相關性事件，Log360即時發出告警與報表



1 At least 5 failed VPN logons in 10 minutes
10分鐘內，5次以上登入VPN失敗

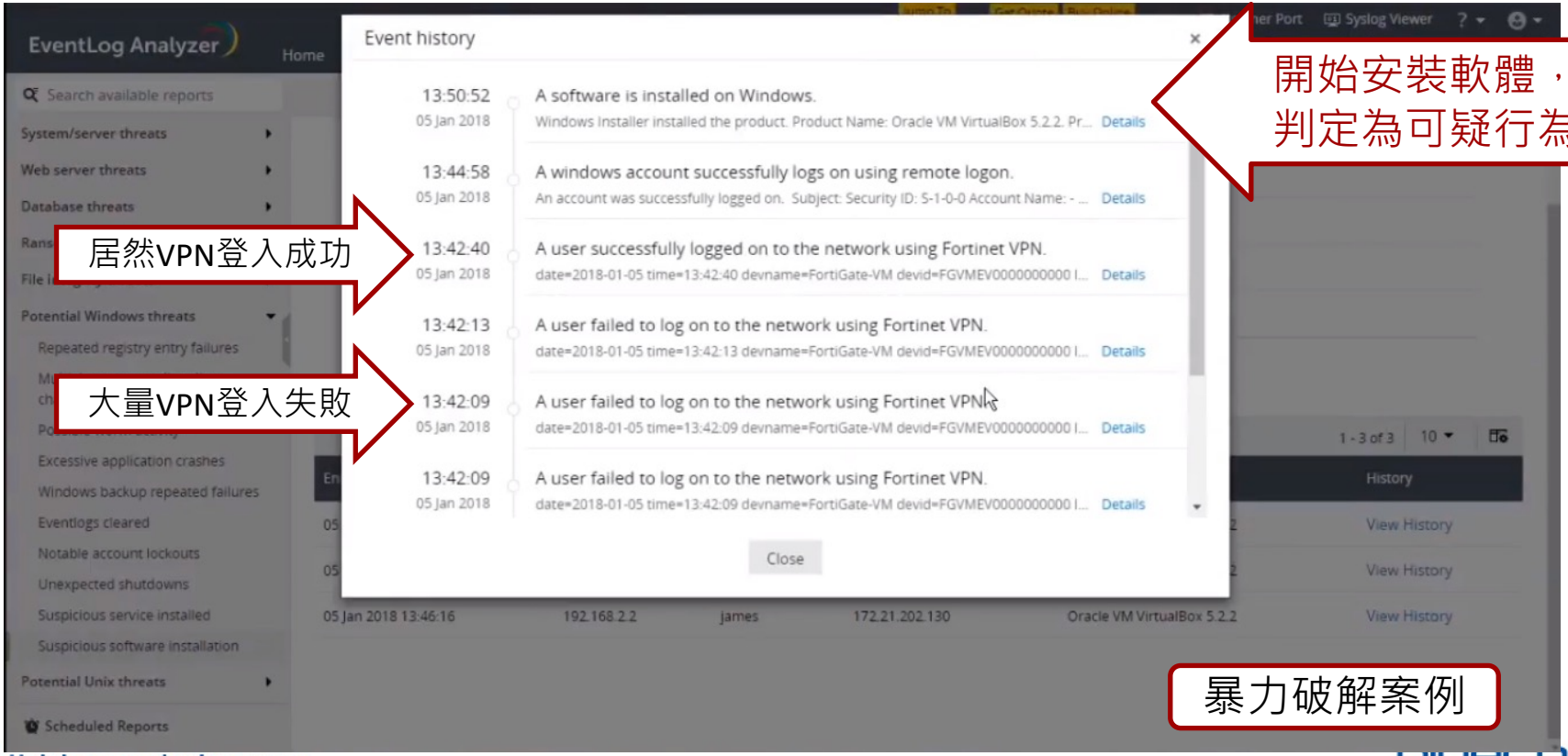
2 Successful VPN logon in next 2 minutes
2分鐘後，登入VPN成功

3 IP address assigned in next 2 minutes
取得內部IP

4 Successful remote logon to target device in next 15 minutes
15分鐘後，成功遠端登入目標

5 Malicious software installation in next 30 minutes
30分鐘後，惡意軟體安裝完畢

日誌分析 - 關聯性案例分析



即時事故管理

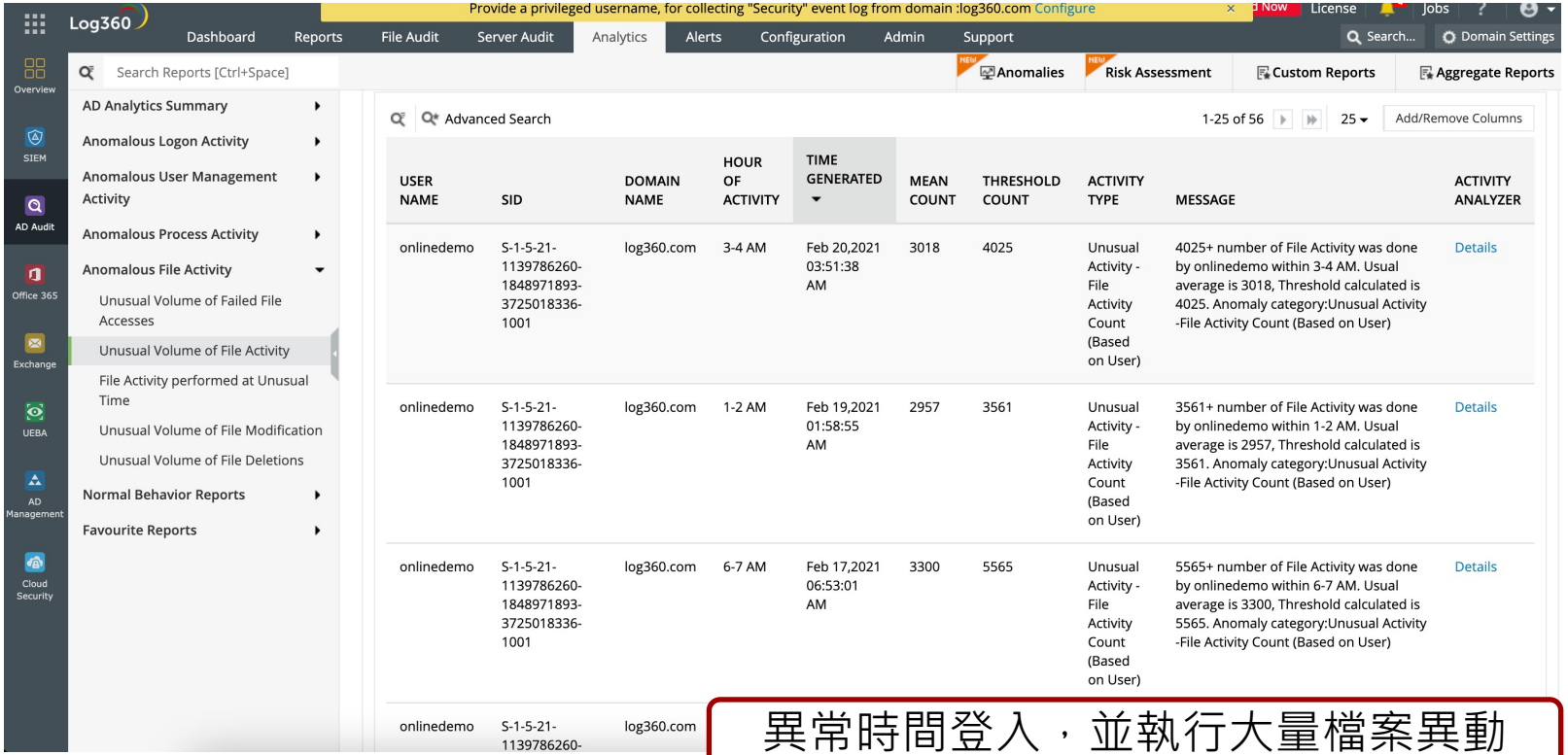
Incident detection and response

何謂資安事故 (security incident)

- 對組織造成威脅的事件(Event)
- 有一定程度的嚴重性和潛在風險。
- 資安事故可能從
  - 網路外部(由駭客發起，例如DDoS、網路釣魚、惡意郵件)
  - 組織內部(濫用特權或身份盜用)

https://www.idx.us/knowledge-center/whats-in-a-name-defining-event-vs-security-incident-vs-data-breach

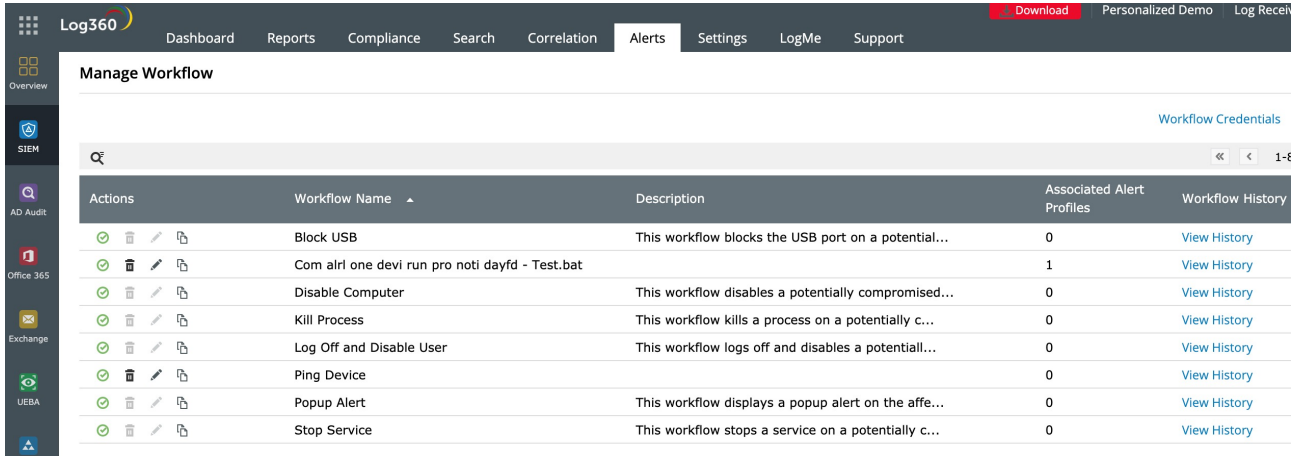
AD行為即時偵測 - 範例

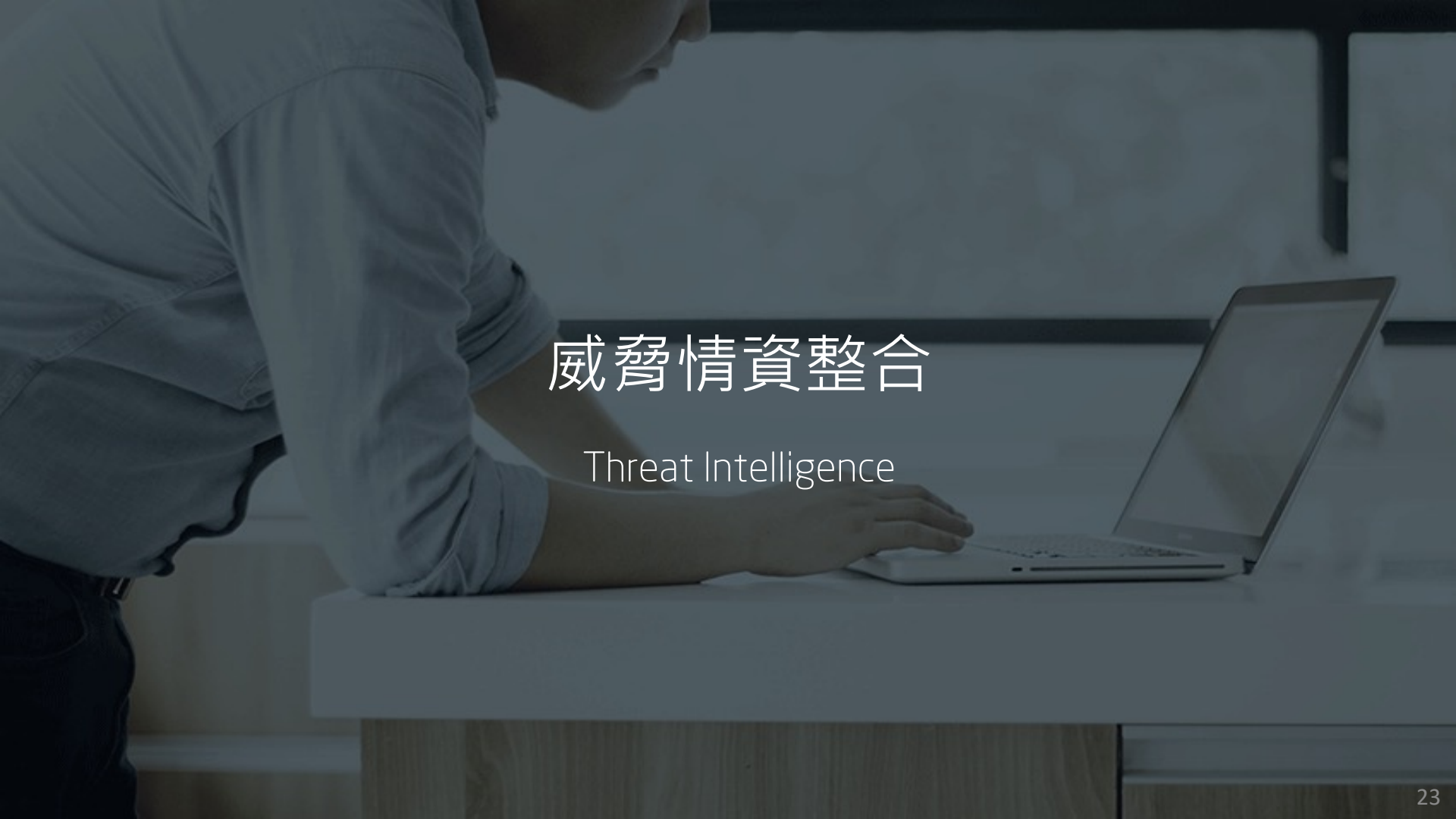


異常時間登入，並執行大量檔案異動

自動回應 - 可自訂因應工作流程

- 不同行為，可自動觸發因應措施
  - 當偵測可疑USB接入，主動阻擋USB使用
  - 偵測使用者不當行為，自動登出並關閉使用者帳戶。

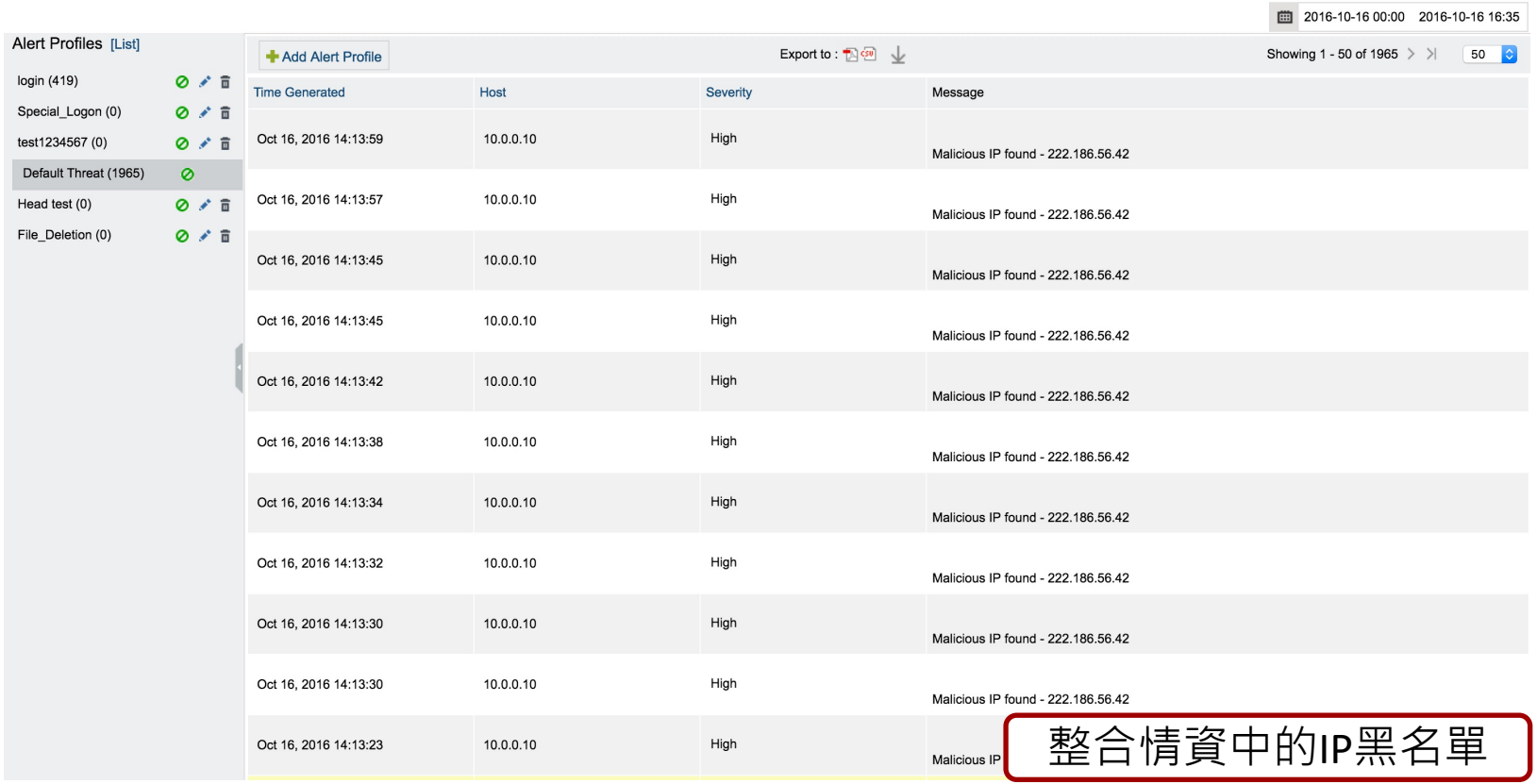



威脅情資整合
Threat Intelligence

威脅情資整合 (Threat intelligence)

- Log360整合多個Open Source(例如AlienVault) STIX / TAXII的威脅情資來源。
- 動態更新超過6億個惡意IP，URL和域名的資料庫。
- 當檢測到可疑IP，URL和域名之間的流量時，即時告警。
- 無需任何預先配置即可設定此功能。

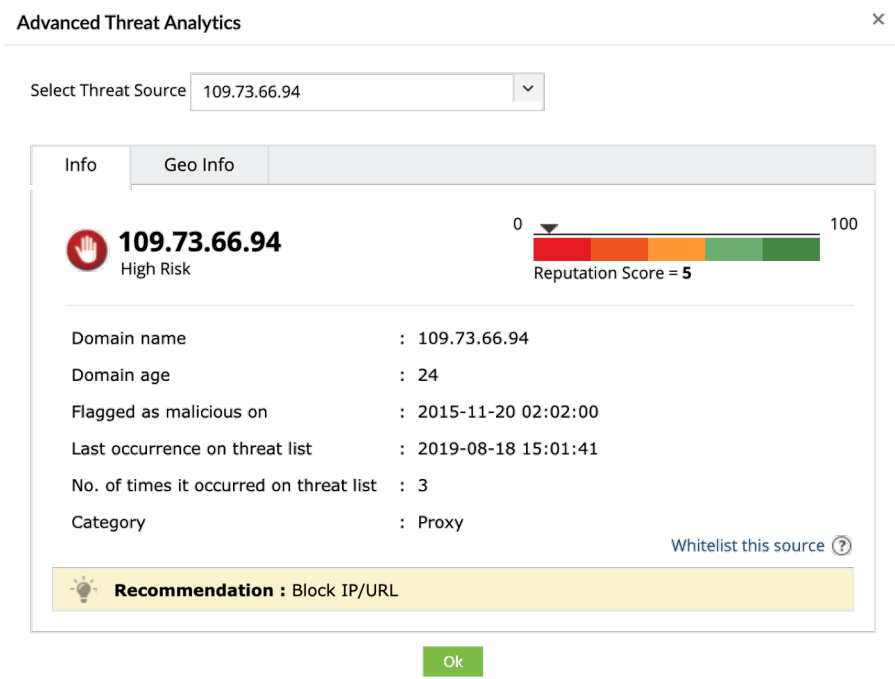
威脅情資整合 - 料敵機先

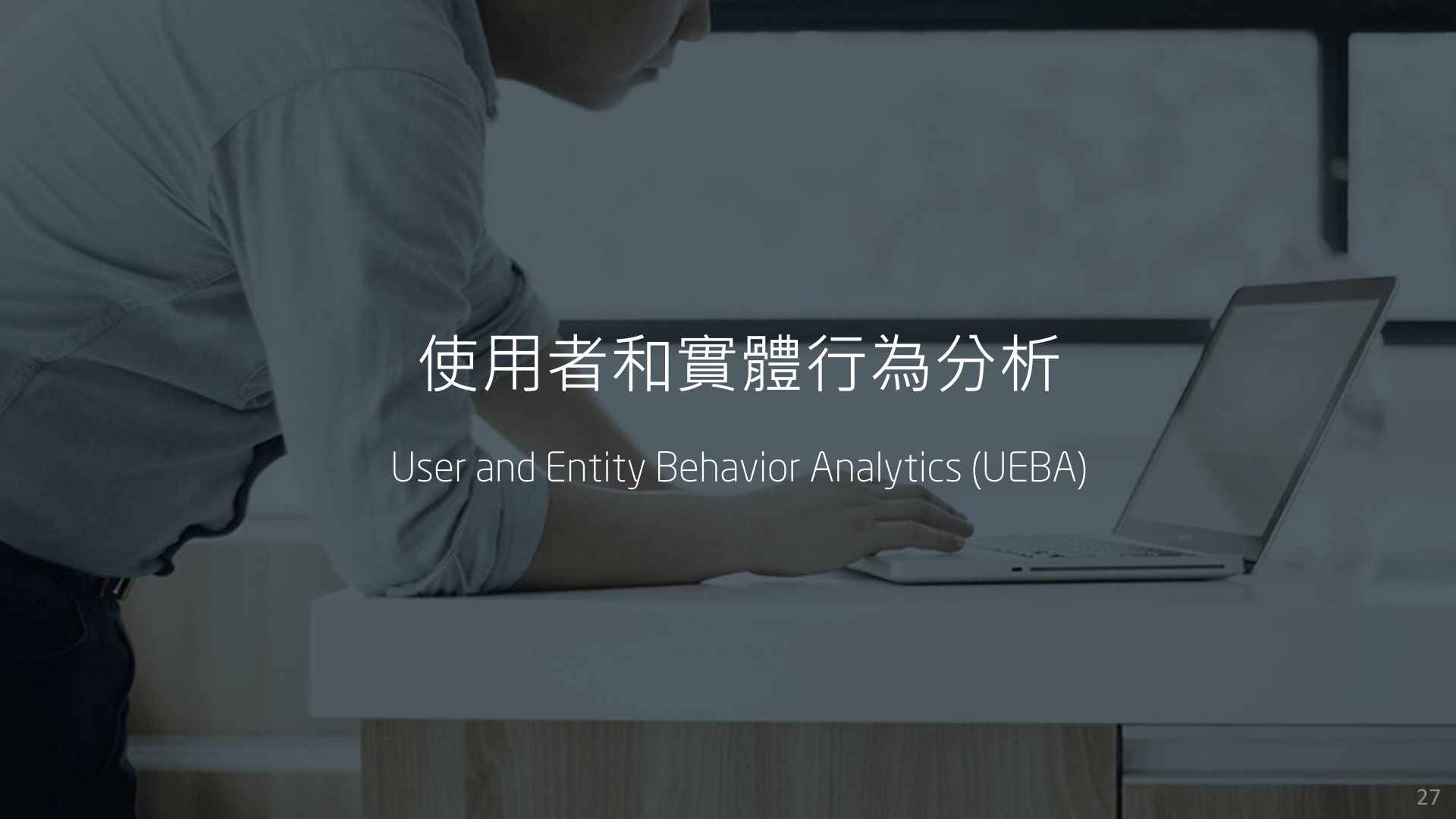


整合情資中的IP黑名單

威脅情資整合 - 料敵機先

- 判斷威脅程度
- 紀錄相關資訊
- 提供最佳建議





使用者和實體行為分析

User and Entity Behavior Analytics (UEBA)

情境應用 - 人物背景

Noah / 台灣區處長 / 46歲
常將帶人要帶心掛在嘴邊，習慣早睡，有領養兩隻米克斯。

Guy / 行銷專員 / 39歲
在Facebook社群裡自稱蓋邊，嗜好是用水波爐烤蛋糕。

Benjamin / 業務協理 / 41歲
有咖啡成癮症，唱歌五音不全，戒菸多年。

NAT / IT系統管理員 / 29歲
專長是網路管理，興趣是收集鋼彈模型，曾交過女友。

情境應用 - 使用軌跡

Noah / 台灣區處長
9~10AM ー 下載20次, 2~3PM ー 下載50次, 5~6AM ー 下載500次

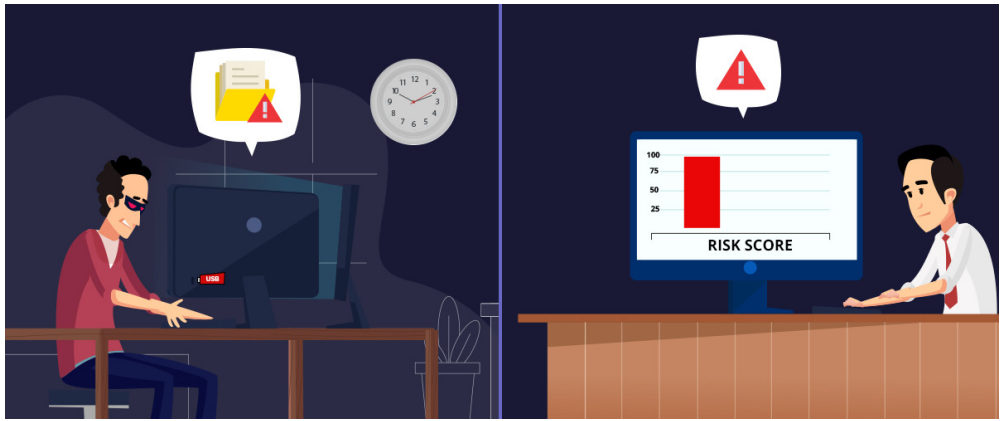
Guy / 行銷專員
昨晚登入到程式碼資源庫並下載了些資料

Benjamin / 業務協理
半夜嘗試登入10幾台機器，並安裝不明應用程式

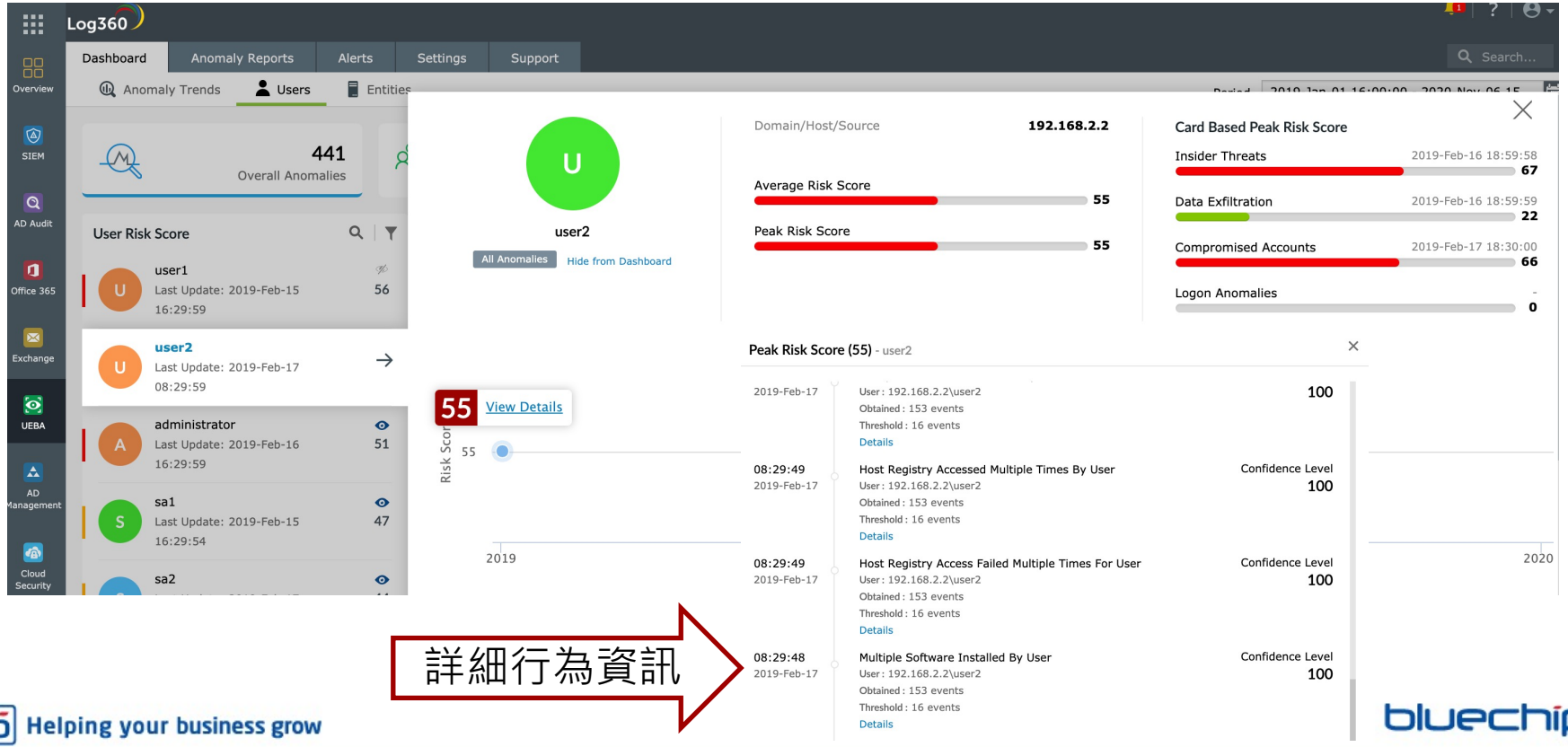
NAT / IT系統管理員
半夜存取了防火牆並修改了DMZ政策

機械學習(ML)與人工智慧(AI)

- 透過ML學習大量異常模式，並透過AI分析正常/異常行為，運算風險指數，例如：
  - 內部威脅
    - 異常時間登入
    - 未經授權的文件存取
  - 帳戶盜用
    - 大量登入失敗
  - 資料外洩
    - 執行異常指令
    - 異常地點登入



使用者行為分析 - 範例



詳細行為資訊

情境應用 - 風險指數

Noah / 台灣區處長 /風險指數 32
9~10AM ー 下載20次, 2~3PM ー 下載50次, 5~6AM ー 下載500次

Guy / 行銷專員 /風險指數 47
昨晚登入到程式碼資源庫並下載了些資料

Benjamin / 業務協理 /風險指數 55
半夜嘗試登入10幾台機器，並安裝不明應用程式

NAT / IT系統管理員 /風險指數 21
半夜存取了防火牆並修改了DMZ政策

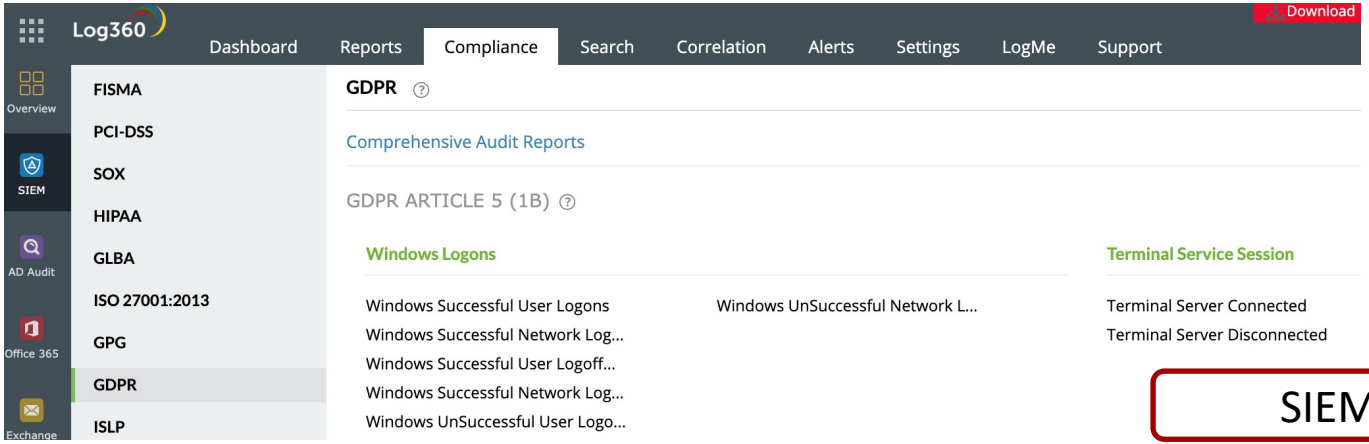
IT合規管理

IT compliance management

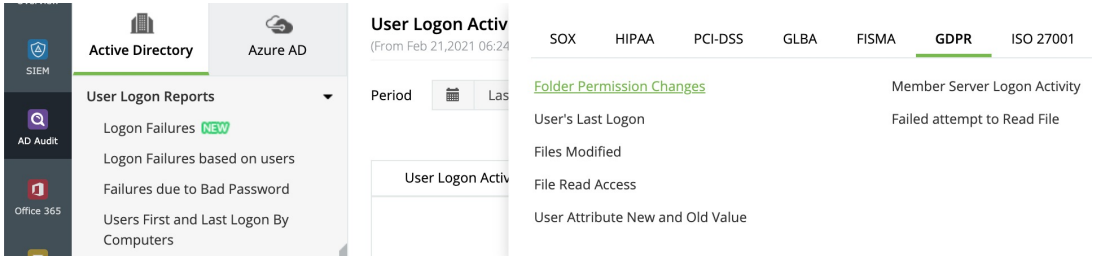
整合合規管理系統

- 產出以下現成合規報表，滿足內部資安策略：
  - PCI DSS / 支付卡產業資料安全標準
  - GDPR / 歐盟個人資料保護規範
  - HIPAA / 美國健康保險流通與責任法案
  - GLBA / 金融服務業現代化法案
  - SOX / Sarbanes-Oxley 法案
  - ISO 27001 / 資訊安全管理國際標準

輕鬆產出合規報表



SIEM 合規報表



AD 合規報表

AD稽核

Active Directory Auditing

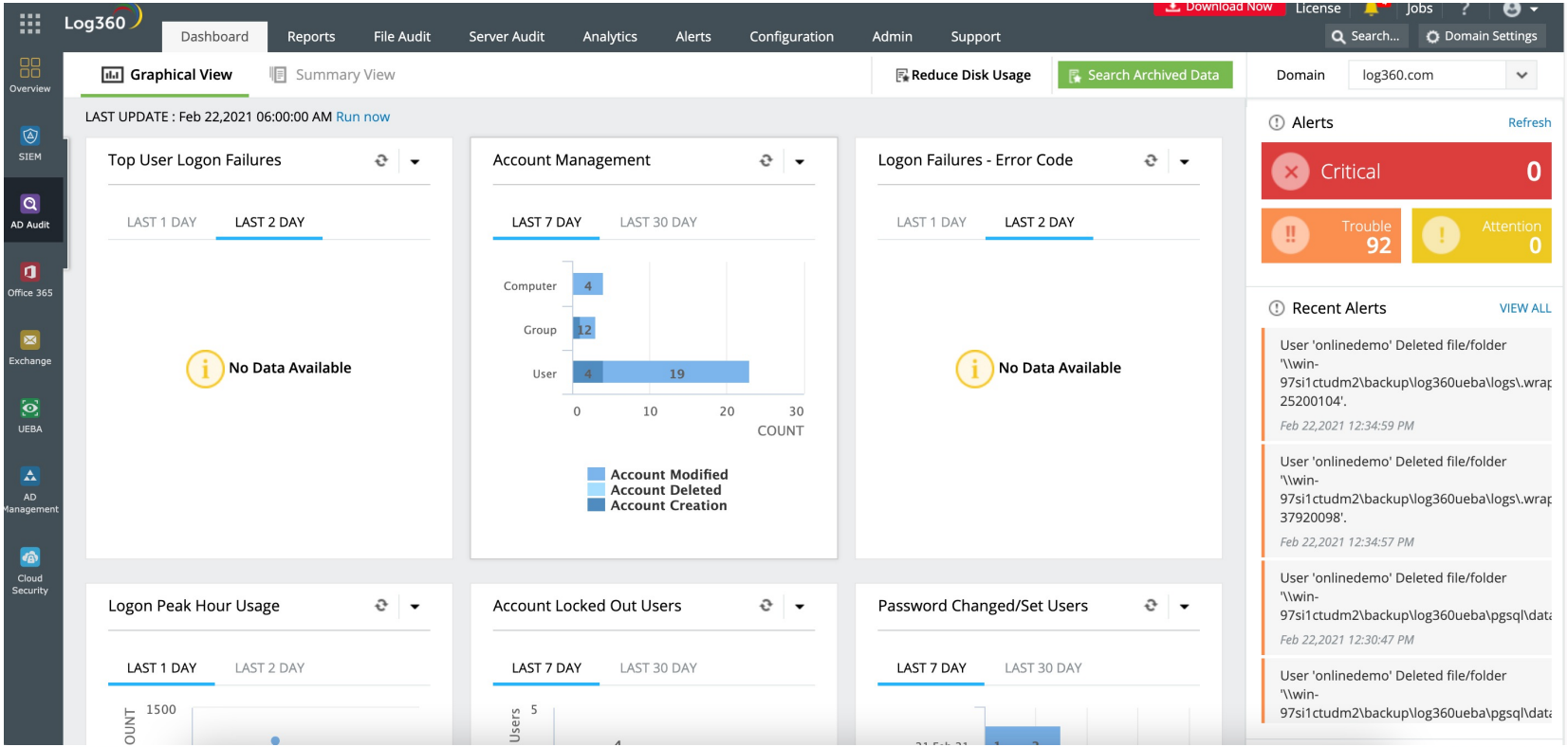
即時稽核 **Active Directory** 變更

- 接收 Active Directory 中任何重大變更的即時警示。
- 透過這些警示和立即可用的報表，Log360 可確保完美的AD稽核和變更監控。
  - 獲取有關 AD 物件的詳細資料
  - 追蹤可疑使用者行為
  - 監控群組和 OU 中的關鍵變更等

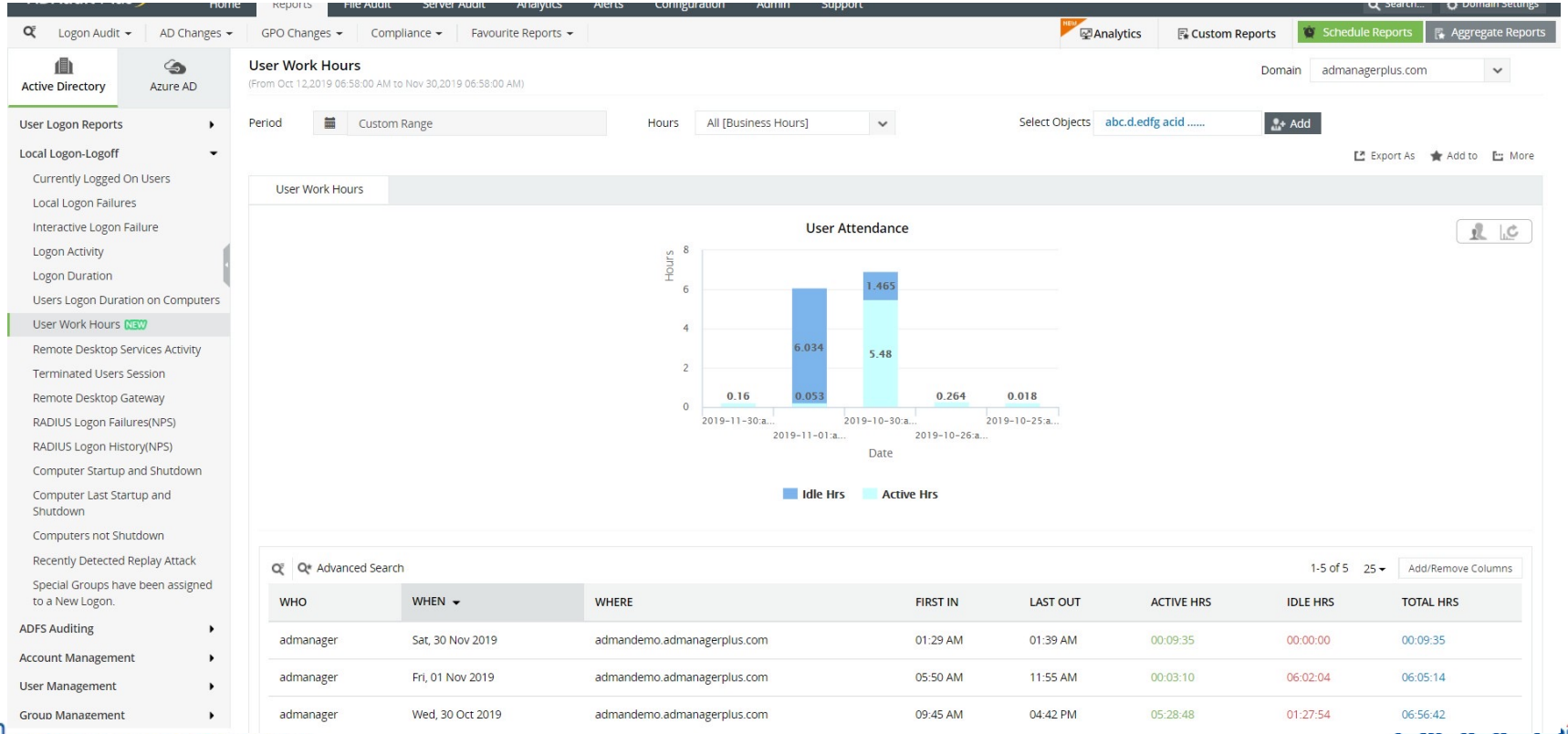
緊密監控 **Active Directory** 物件

- Log360 可以監控您的 AD 環境並提供有關 AD 物件的詳盡報表，突出顯示相關重要安全資訊
  - 使用者
  - 電腦
  - 安全群組
  - GPO
  - OU
  - 檔案/資料夾等

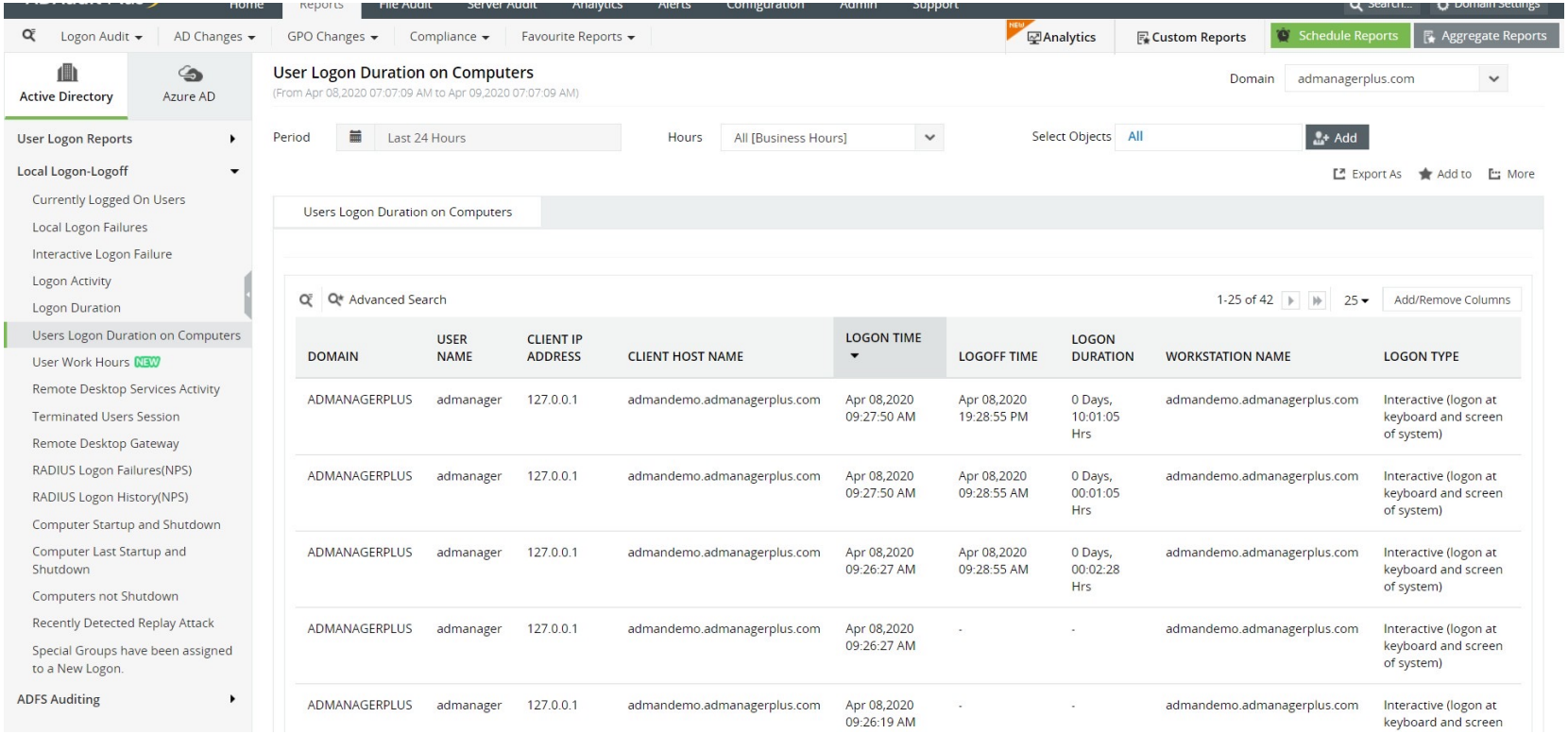
AD稽核管理 - 介面範例


Log360
Dashboard
Reports
File Audit
Server Audit
Analytics
Alerts
Configuration
Admin
Support
Download Now
License
Jobs
Search...
Domain Settings
Overview
SIEM
AD Audit
Office 365
Exchange
UEBA
AD Management
Cloud Security
Graphical View
Summary View
Reduce Disk Usage
Search Archived Data
Domain
log360.com
LAST UPDATE : Feb 22,2021 06:00:00 AM Run now
Top User Logon Failures
LAST 1 DAY
LAST 2 DAY
No Data Available
Account Management
LAST 7 DAY
LAST 30 DAY
Computer
Group
User
4
12
4
19
0
10
20
30
COUNT
Account Modified
Account Deleted
Account Creation
Logon Failures - Error Code
LAST 1 DAY
LAST 2 DAY
No Data Available
Alerts
Refresh
Critical
0
Trouble
92
Attention
0
Recent Alerts
VIEW ALL
User 'onlinedemo' Deleted file/folder '\\win-97si1ctudm2\backup\log360ueba\logs\.wrap 25200104'.
Feb 22,2021 12:34:59 PM
User 'onlinedemo' Deleted file/folder '\\win-97si1ctudm2\backup\log360ueba\logs\.wrap 37920098'.
Feb 22,2021 12:34:57 PM
User 'onlinedemo' Deleted file/folder '\\win-97si1ctudm2\backup\log360ueba\pgsql\data
Feb 22,2021 12:30:47 PM
User 'onlinedemo' Deleted file/folder '\\win-97si1ctudm2\backup\log360ueba\pgsql\data
Logon Peak Hour Usage
LAST 1 DAY
LAST 2 DAY
1500
Account Locked Out Users
LAST 7 DAY
LAST 30 DAY
5
Password Changed/Set Users
LAST 7 DAY
LAST 30 DAY

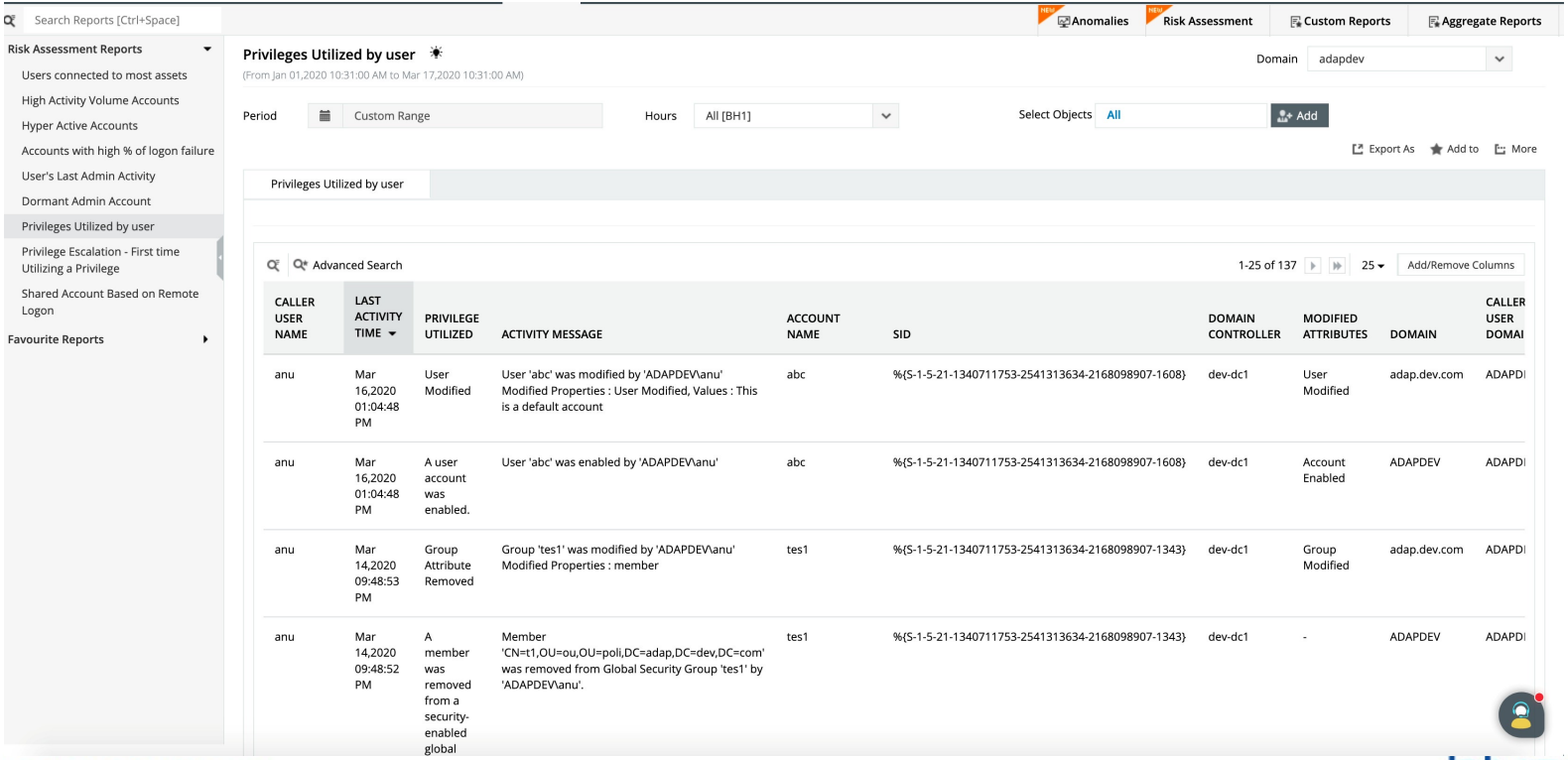
AD稽核管理 - 使用者上線時間報表



AD稽核管理 - 使用者登入操作軌跡

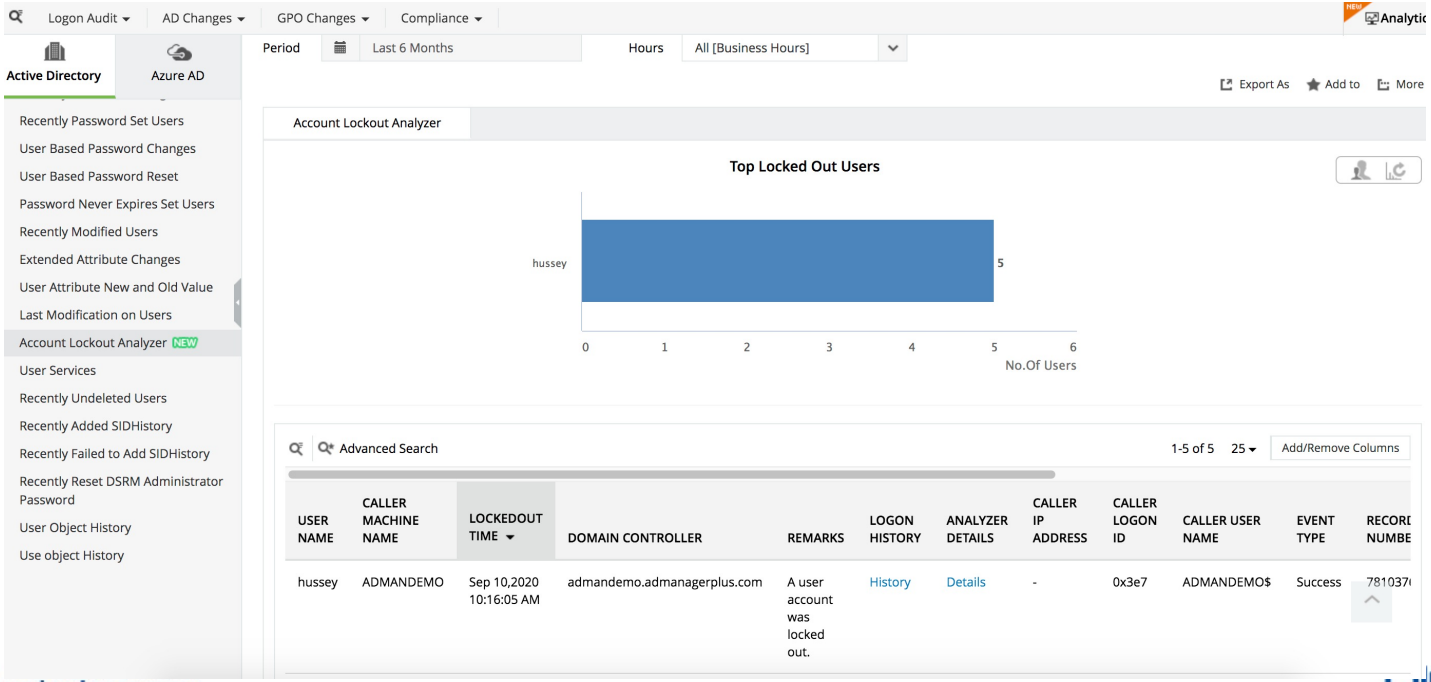


AD稽核管理 - 異常登入資安事件報表

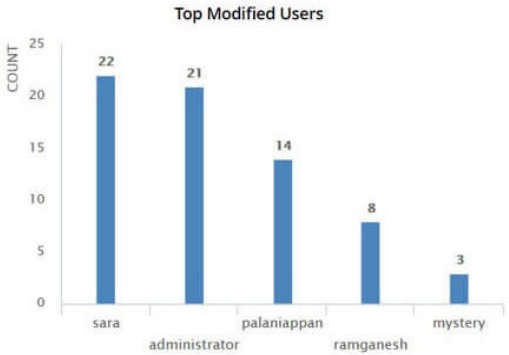


使用情境 - 最常被暴力破解的帳戶

- 常常被鎖住的帳號，往往都是惡意存取的目標



使用情境 - 特權使用者行為監控



1-25 of 70 | 25 | Add/Remove Columns

MODIFIED TIME	DOMAIN CONTROLLER	MESSAGE	WHO CHANGED	MODIFIED ATTRIBUTES	NEW VALUE	OLD VALUE	REMARKS
Jul 05,2016 05:46:59 PM	ADAP-DC1	Group Policy Object 'adap_ADAuditPlusPolicy' was modified by 'ADAP\administrator'. Modified Properties : NT-Security-Descriptor	administrator	NT-Security-Descriptor	New ACL More	Old ACL More	Write Property : groupPolicyContainer More
Jul 05,2016 04:50:13 PM	ADAP-DC1	Group Policy Object 'adap.internal.com_ADAuditPlusPolicy' was modified by 'ADAP\saravanan.nagarajan'. Modified Properties : NT-Security-Descriptor	saravanan.nagarajan	NT-Security-Descriptor	New ACL More	Old ACL More	Write Property : groupPolicyContainer More


公有雲日誌管理
A comprehensive cloud log management solution

整合各大雲平台


Azure log monitoring
AWS log monitoring
Salesforce
User Activity
Securing Google
Cloud Platform

Microsoft Azure

日誌來源	說明
Azure 活動記錄	活動記錄是 Azure 中的平臺記錄 ，可提供訂用帳戶層級事件的見解。 這包括修改資源或啟動虛擬機器時的資訊。
網路安全性群組流量記錄	流量記錄是 Azure 網路監看員的一項功能，可讓您記錄流經 NSG 之 IP 流量的相關資訊。 流量資料會傳送Cloud Security Plus。

Amazon Web Services (AWS)

日誌來源	說明
AWS CloudTrail	CloudTrail 可以記錄、持續監控和保留 AWS 基礎設施中所有與動作相關的帳戶活動。
Server access logging	當您啟用Server access logging時，Amazon S3 會為來源儲存貯體，提供存取日誌給您所選擇的目標儲存貯體。
Elastic Load Balancing Access logs	Elastic Load Balancing 提供存取日誌，可針對傳送到負載平衡器的請求，擷取其詳細資訊。

Google Cloud Platform

日誌來源	說明
Cloud Audit Logging	Cloud Audit Logs 為每個 Google Cloud 專案、資料夾和組織維護三種審核日誌：管理員活動、資料存取和系統事件。 Google Cloud 服務會將稽核資訊寫入這些日誌，以說明在您的資源中，哪些使用者在何時何處，執行了什麼操作。

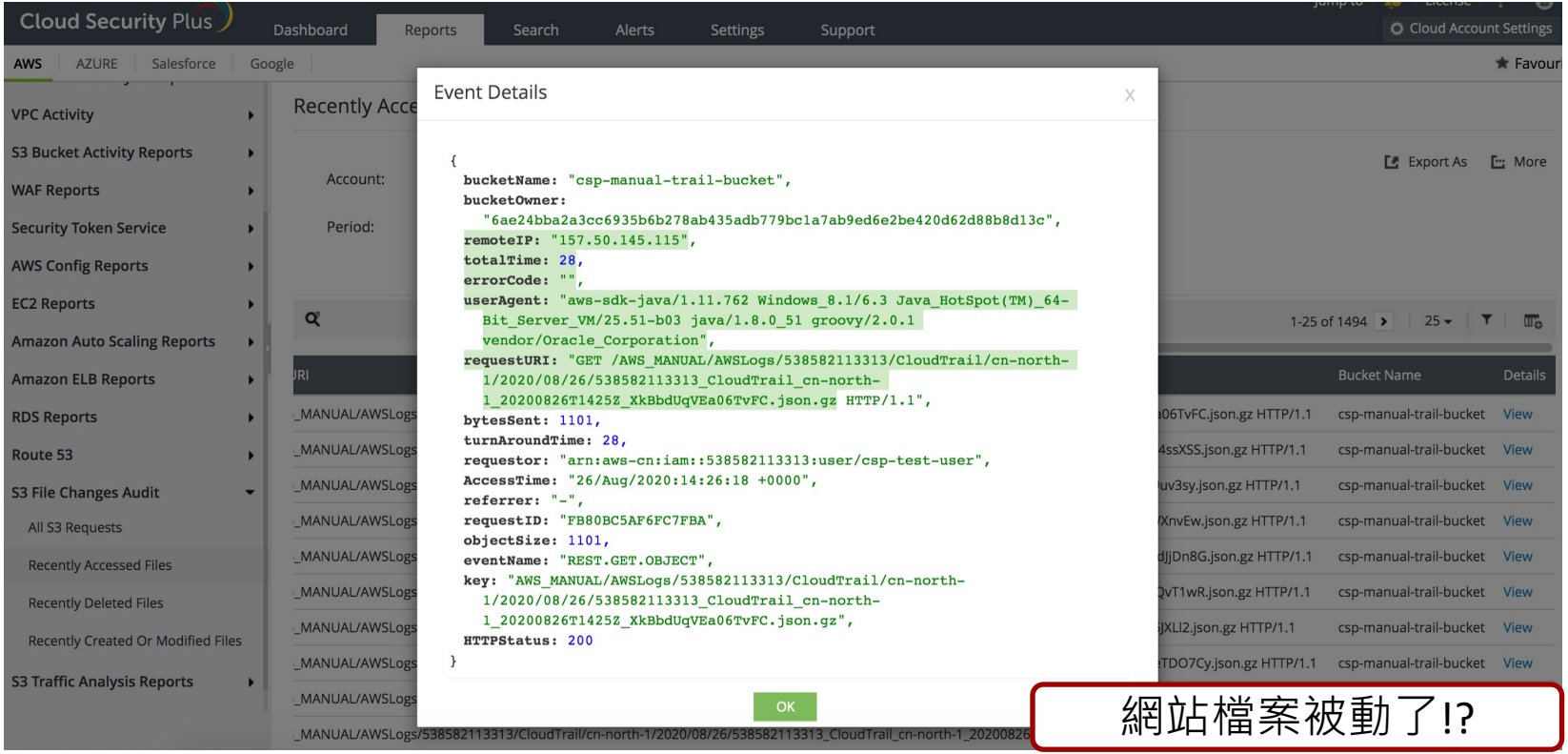
使用情境

AWS運作之內部資安事件

- S3的檔案被異動了!
  - 異常的外部存取S3。

- Cloud Security Plus 可以提供什麼協助?
  - 透過”S3 File Change Audit – Recent Accessed Files”報表查詢哪些S3上的檔案被異動，包含來源IP/User Agent等資訊
  - 可設定告警提醒管理員

AWS S3 上，時間點/存取IP/存取路徑

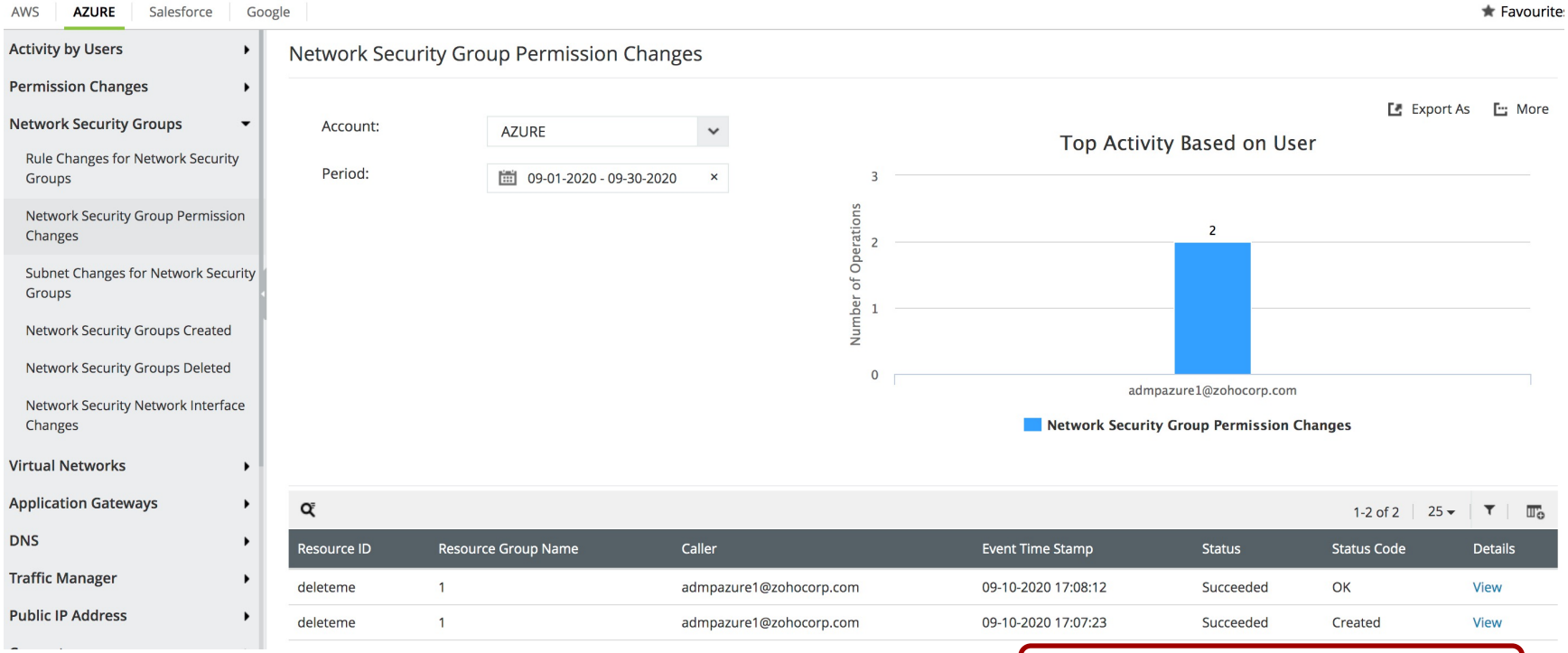


Azure 網路內部資安事件

- 網路安全群組上的規則改變了!
  - 內部人員改變網路安全群組，允許未知存取進來

- Cloud Security Plus 可以提供什麼協助?
  - 透過報表了解，變更了哪些網路安全群組、權限變更、子網域變更等等。
  - 並設定告警提醒管理員

Azure上，時間點/帳號/網路安全群組權限變更

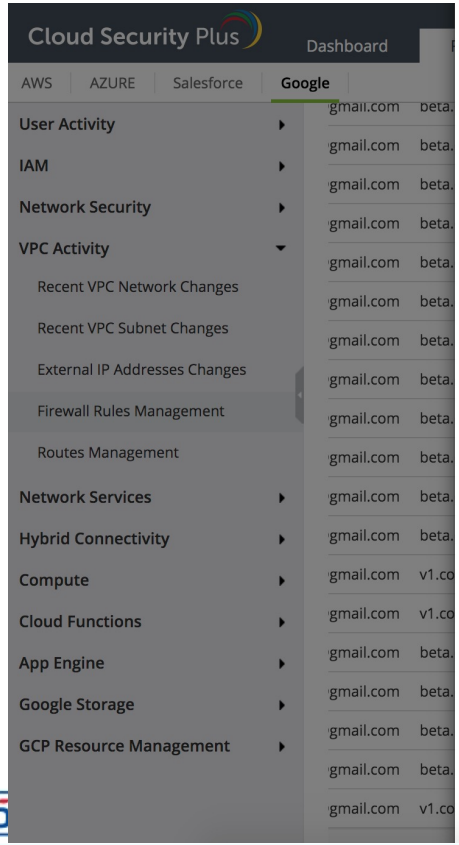


安全群組權限被改了!?

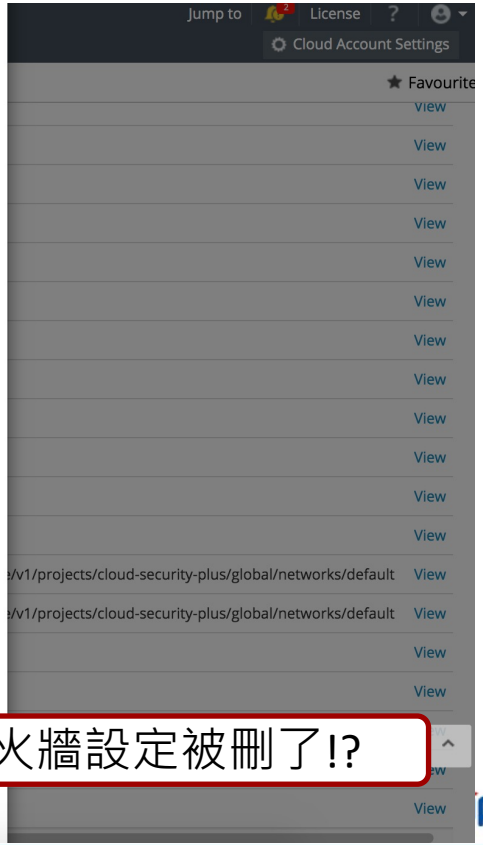
目前還在進化中

- 未來將開發更多功能，包括：
- 稽核更多AWS服務
  - CloudFront, VPC Flow, RDS, Lambda, Glacier, DynamoDB, Redshift, Elastic Beanstalk, Kinesis
- 稽核更多Azure服務
  - Web Apps, Content Delivery Network, Storage Analytics, Data Lake, Data Factory

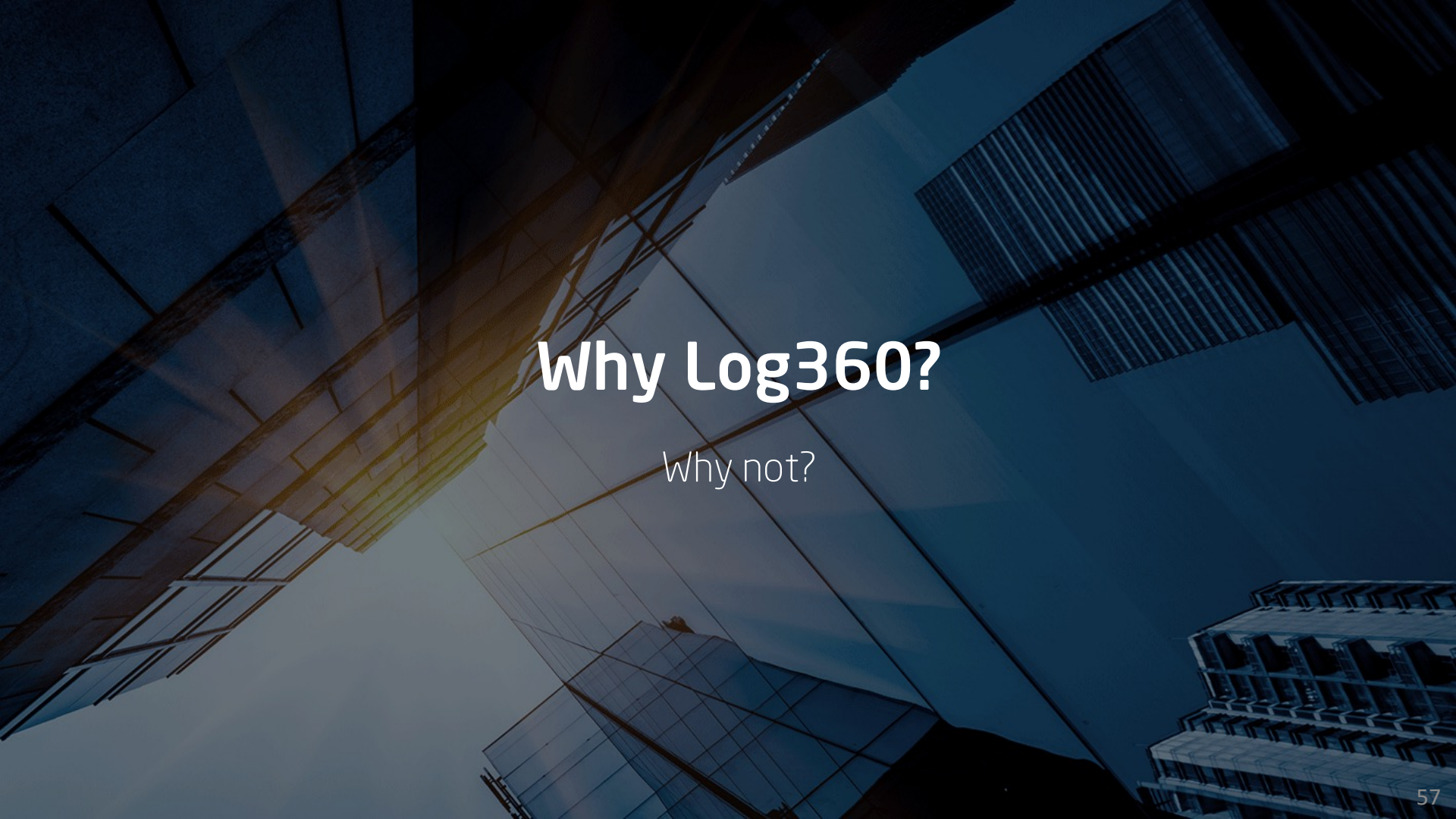
GCP上，時間點/帳號/IP/刪除防火牆設定




```
+ resource: {"type":"gce_firewall_rule","labels":{"project… },
- protoPayload:
  {
    - requestMetadata:
      {
        + requestAttributes: {"reason":"8uSywAY4GjZGb3IgYmFja2dyb3VuZCBvcGV… },
        + destinationAttributes: {},
        callerSuppliedUserAgent: "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
          AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.30
          Safari/537.36,gzip(gfe),gzip(gfe)",
        callerIp: "182.74.243.42"
      }
    + request: {"@type":"type.googleapis.com/compute.firewall… },
    + authenticationInfo: {"principalEmail":"mydeenmnk@gmail.com"},
    + authorizationInfo: [{"permission":"compute.firewalls.delete","res… ],
    @type: "type.googleapis.com/google.cloud.audit.AuditLog",
    - response:
      {
        targetId: "9128318253791671780",
        @type: "type.googleapis.com/operation",
        selfLink: "https://www.googleapis.com/compute/v1/projects/cloud-
          security-plus/global/operations/operation-159..",
        insertTime: "2020-09-10T17:59:24.636-07:00",
        selfLinkWithId: "https://www.googleapis.com/compute/v1/projects/cloud-
          security-plus/global/operations/6850173948231..",
        targetLink: "https://www.googleapis.com/compute/v1/projects/cloud-
          security-plus/global/firewalls/mnk-rule",
        name: "operation-1599785964290-5aeff321e4010-17c0e0c8-d77bfac5",
        progress: "0",
        operationType: "delete",
        startTime: "2020-09-10T17:59:24.645-07:00",
        id: "6850173948231382275",
        user: "mydeenmnk@gmail.com",
        status: "RUNNING"
      }
    - resourceOriginalState:
```

防火牆設定被刪了!?


Why Log360?
Why not?

連續四屆入圍

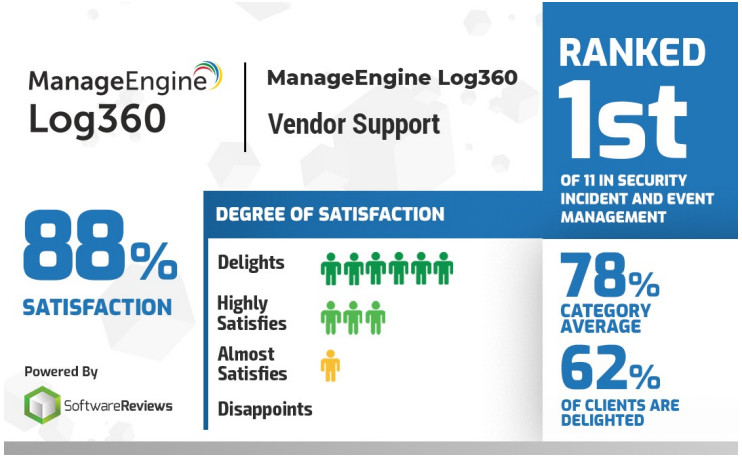
Gartner Magic Quadrant for Security Information and Event Management (2016-2018/2020)

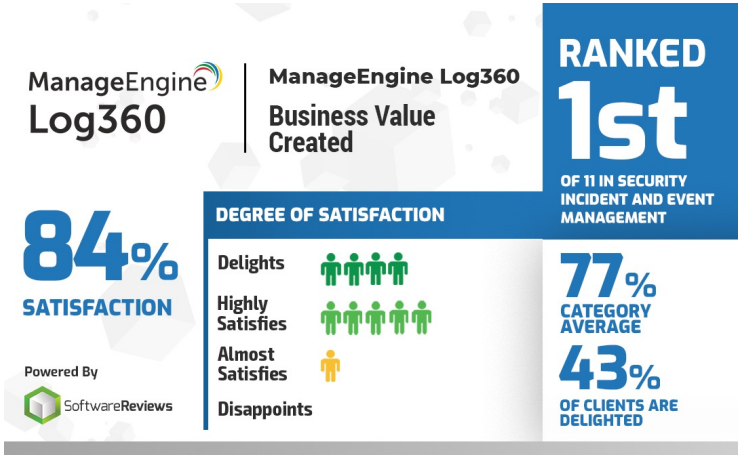
#2019並無出刊

Figure 1. Magic Quadrant for Security Information and Event Management

Source: Gartner (February 2020)

Software Reviews' SIEM 客戶體驗報告中奪得冠軍 (2019)





選擇 Log360

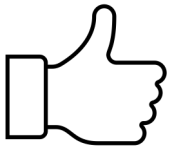
- 五分鐘安裝完畢，簡單管理，支援絕大部分日誌來源
- 結合威脅情資，與使用者行為分析，快速因應資安風險
- 預設合規報表，輕鬆滿足合規需求
- 極具競爭力的價格

最小安裝環境

- CPU：3G / 8 cores
- RAM：16GB
- Disk space：300 GB
- Windows Server 2012/2016/2019

直接線上試用**DEMO**吧!

http://log360demo.manageengine.com/



也可以先試試免費版的

為你呈現

ManageEngine

Introduing ManageEngine

全方位IT管理解決方案

- IT整合管理
  - 提供 90 多種，價格合理，滿足您的所有 IT 管理需求之產品。
- IT簡化管理
  - 易於下載、安裝、設定和部署，無需第三方支援服務或幫助。
- IT實惠管理
  - 更高的價格並不始終意味著更好的產品

180,000+
家全球企業

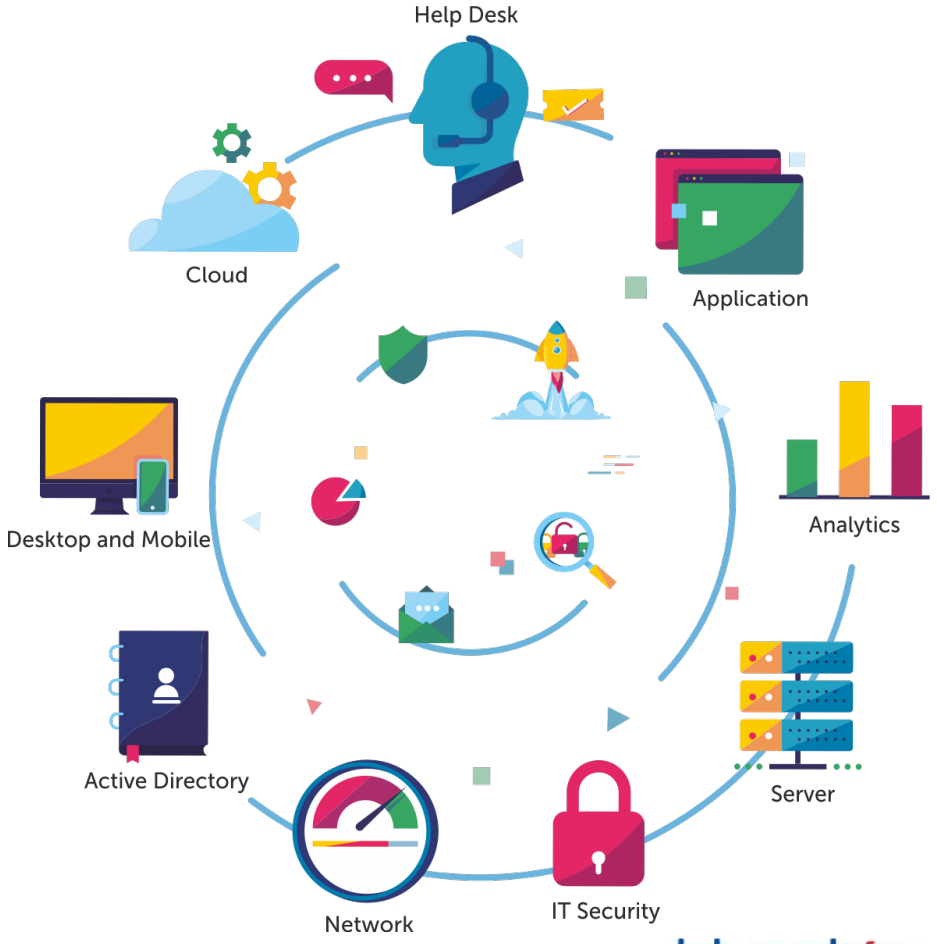
9/10
財富 100 強公司

3,000,000+
管理者

..信任 ManageEngine 來管理其 IT。

ManageEngine 協助您

- ITIL整合式資產和服務管理
- 更有效的管理雲平台
- 比讓微軟更實用的AD管理
- 大量端末設備
- 複雜的基礎設施
- 符合資安需求的稽核
- 可滿足所有IT管理需求



THANK YOU

Any Questions?

Or

Contact Kerry