

ManageEngine

Log360

全方位 SIEM & AD

日誌與資安事件分析管理系統

bluechip
infotech



11 JAN 2021 NEWS

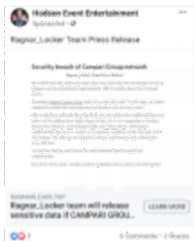
Over 100,000 UN Employee Records Accessed by Researchers

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



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

Enters the wrong password **240**
times in a minute. (Logon failure,
event ID 4625)

輸入密碼錯誤，一分鐘超過240次



Enters the right password after
240 attempts. (**Logon success**,
event ID 4624)

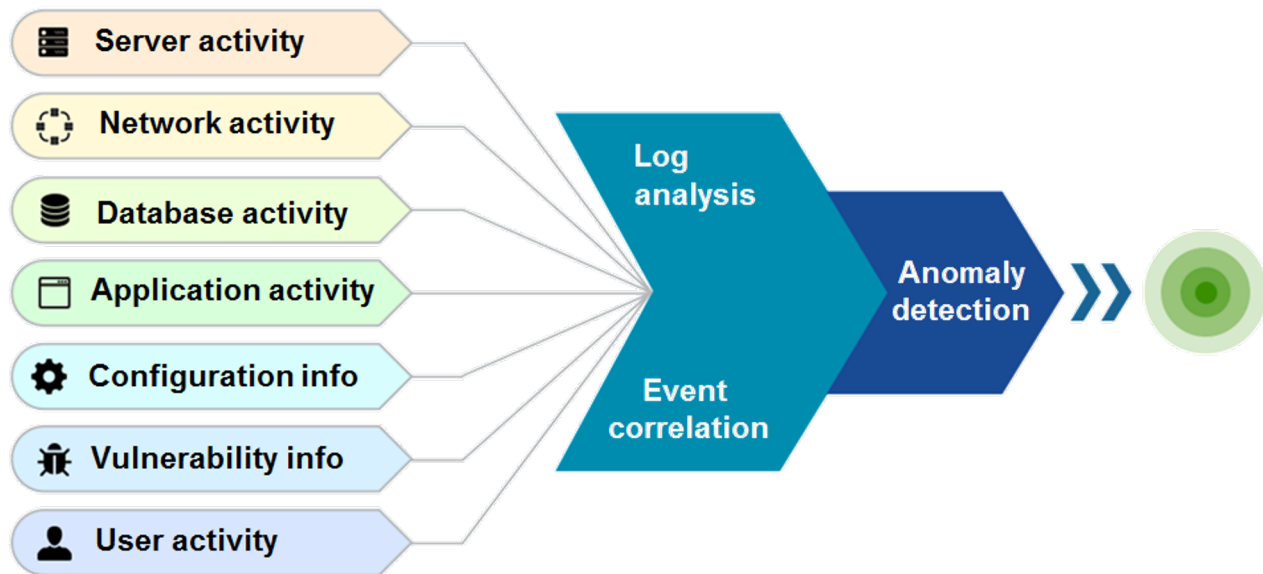
240次嘗試登入後，登入成功

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



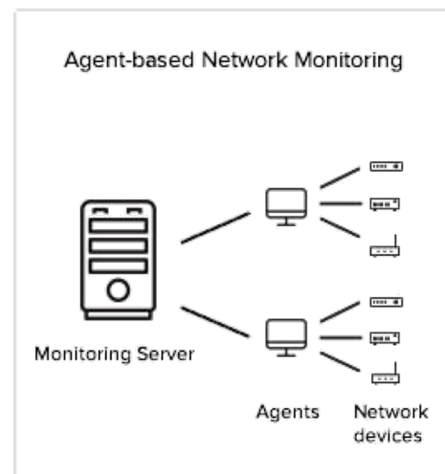
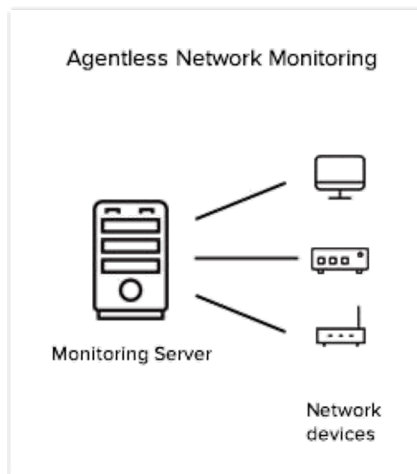
A person in a light blue shirt is sitting at a white desk, working on a laptop. The scene is dimly lit, with the person's face partially visible in profile. The background is a blurred office environment.

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

Log360 Dashboard

Log Sources

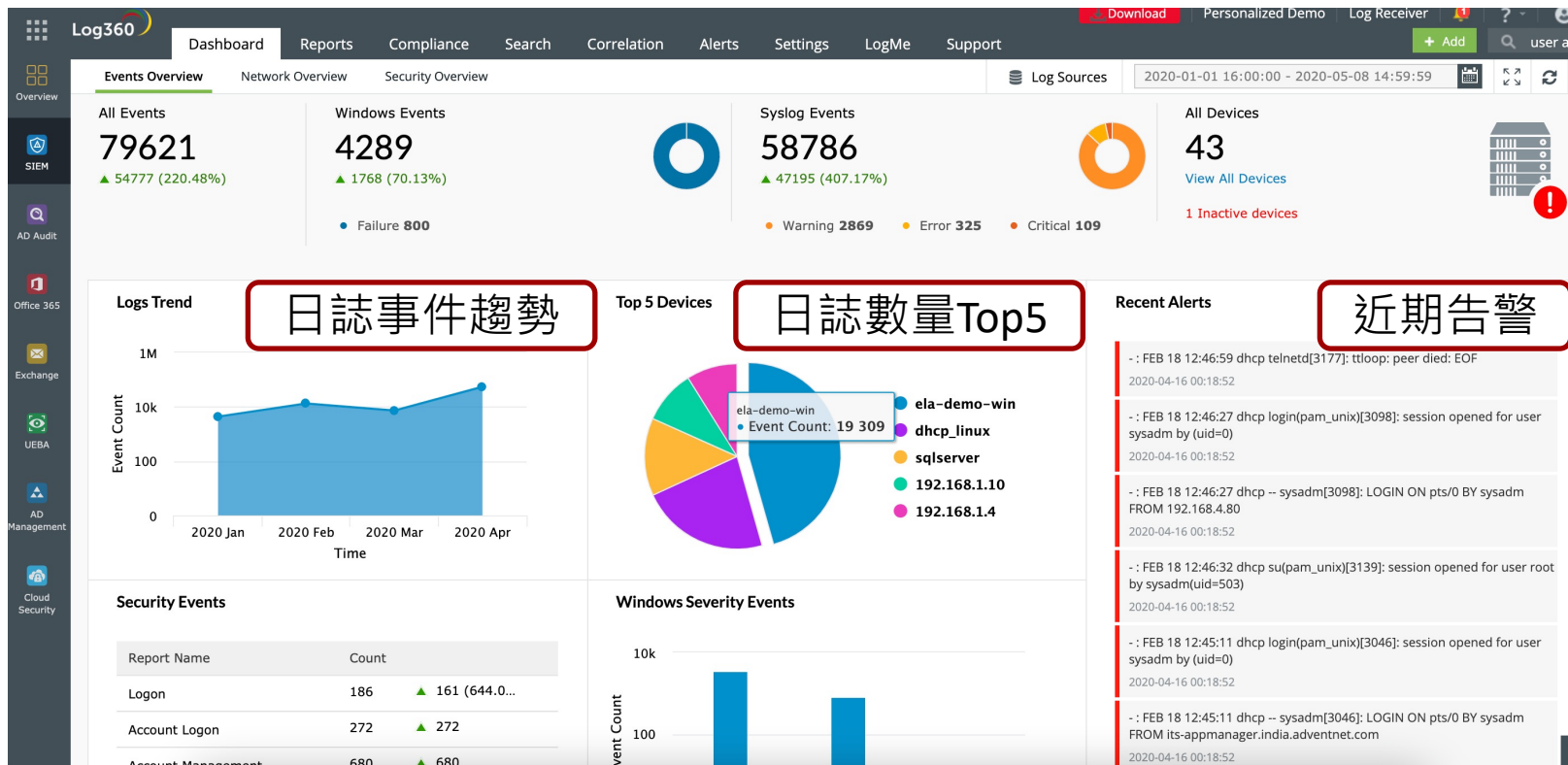
Device(s)	Applications	File Integrity Monitoring						
Device	Show IP	Event Count	[Hide]	Error	Failure	Warning	Others	Last Message Time
WIN-SERVER-2012	Windows	2504		0	800	0	1704	2020-04-08 00:20:01
WIN-SERVER-2012	Windows	0		0	0	0	0	2018-07-02 18:43:05
WATCHGUARD	WatchGuard	3888		55	0	1092	2741	-
UNIX-TWO	Linux	0		0	0	0	0	2017-09-07 00:15:15
UNIX-THREE	Linux	0		0	0	0	0	2017-09-07 00:15:15
UNIX-ONE	Linux	0		0	0	0	0	2017-09-01 13:18:23 [Last 10 Events]
SYMANTEC-SERVER	Symantec	0		0	0	0	0	2017-09-07 00:15:15
SQLSERVER	Microsoft SQL Server	0		0	0	0	0	2017-08-31 16:23:21
SQLSERVER	Microsoft SQL Server	0		0	0	0	0	2017-09-27 20:49:04
SOPHOS	Sophos	0		0	0	0	0	2018-10-01 11:29:05
SONICWALL	SonicWall	19309		128	0	2801	16380	2020-04-14 01:16:57

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

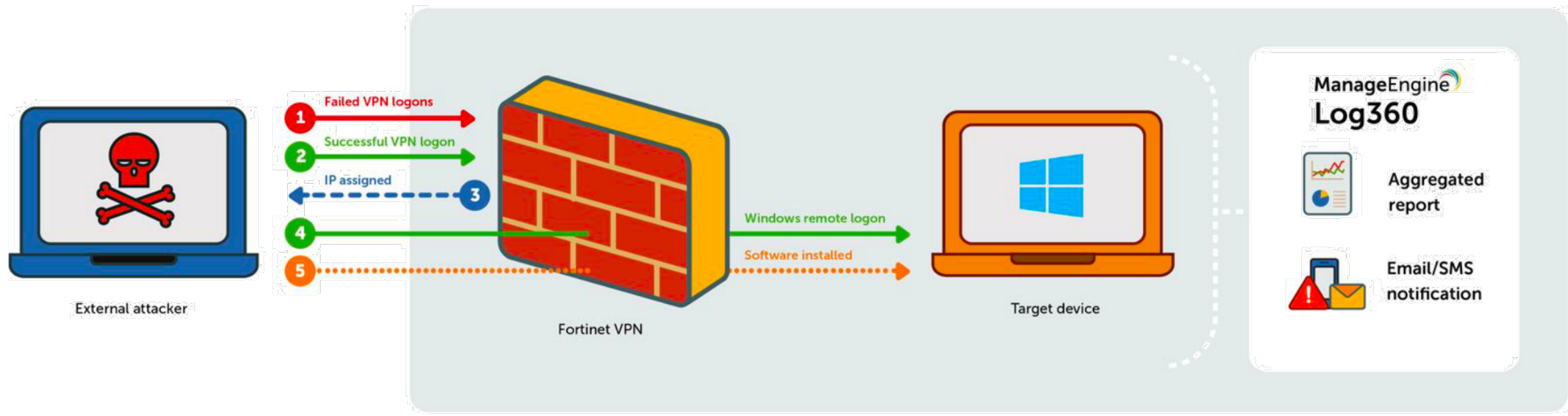


日誌分析 - 關聯性分析

- 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

Suspicious software installations



- 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

The screenshot displays the EventLog Analyzer interface. The main window shows an event history list with the following entries:

Time	Event Description
13:50:52 05 Jan 2018	A software is installed on Windows. Windows Installer installed the product. Product Name: Oracle VM VirtualBox 5.2.2. Pr... Details
13:44:58 05 Jan 2018	A windows account successfully logs on using remote logon. An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - ... Details
13:42:40 05 Jan 2018	A user successfully logged on to the network using Fortinet VPN. date=2018-01-05 time=13:42:40 devname=FortiGate-VM devid=FGVMEV0000000000 L... Details
13:42:13 05 Jan 2018	A user failed to log on to the network using Fortinet VPN. date=2018-01-05 time=13:42:13 devname=FortiGate-VM devid=FGVMEV0000000000 L... Details
13:42:09 05 Jan 2018	A user failed to log on to the network using Fortinet VPN. Details
13:42:09 05 Jan 2018	A user failed to log on to the network using Fortinet VPN. date=2018-01-05 time=13:42:09 devname=FortiGate-VM devid=FGVMEV0000000000 L... Details

Annotations on the screenshot:

- A red arrow points to the 13:42:40 event with the text: 居然VPN登入成功 (Surprisingly VPN login successful).
- A red arrow points to the 13:42:09 event with the text: 大量VPN登入失敗 (Large number of VPN login failures).
- A red arrow points to the top right of the event history window with the text: 開始安裝軟體，判定為可疑行為 (Start installing software, judged as suspicious behavior).
- A red box at the bottom right contains the text: 暴力破解案例 (Brute force case).

A person in a light blue shirt is shown from the side, leaning over a white desk and working on a laptop. The scene is dimly lit, with the person's face and hands visible against the dark background. The laptop is open and positioned on the right side of the desk.

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)



AD行為即時偵測 - 範例

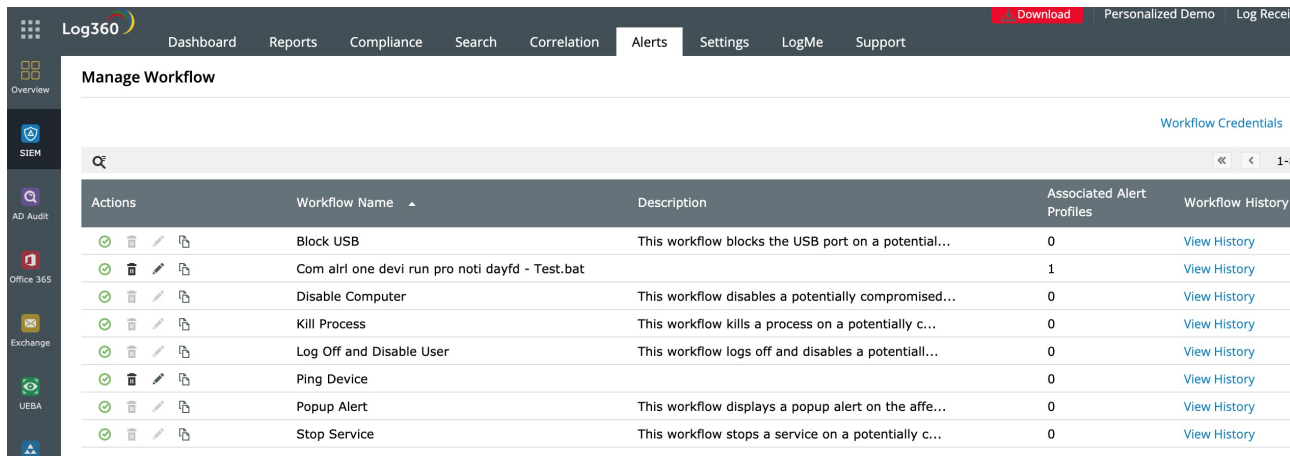
The screenshot displays the Log360 SIEM interface. The top navigation bar includes 'Dashboard', 'Reports', 'File Audit', 'Server Audit', 'Analytics', 'Alerts', 'Configuration', 'Admin', and 'Support'. The left sidebar lists various report categories such as 'AD Analytics Summary', 'Anomalous Logon Activity', 'Anomalous User Management Activity', 'Anomalous Process Activity', 'Anomalous File Activity', and 'Normal Behavior Reports'. The main content area shows an 'Advanced Search' results table with the following data:

























USER NAME	SID	DOMAIN NAME	HOUR OF ACTIVITY	TIME GENERATED	MEAN COUNT	THRESHOLD COUNT	ACTIVITY TYPE	MESSAGE	ACTIVITY ANALYZER
onlinedemo	S-1-5-21-1139786260-1848971893-3725018336-1001	log360.com	3-4 AM	Feb 20,2021 03:51:38 AM	3018	4025	Unusual Activity - File Activity Count (Based on User)	4025+ number of File Activity was done by onlinedemo within 3-4 AM. Usual average is 3018, Threshold calculated is 4025. Anomaly category:Unusual Activity -File Activity Count (Based on User)	Details
onlinedemo	S-1-5-21-1139786260-1848971893-3725018336-1001	log360.com	1-2 AM	Feb 19,2021 01:58:55 AM	2957	3561	Unusual Activity - File Activity Count (Based on User)	3561+ number of File Activity was done by onlinedemo within 1-2 AM. Usual average is 2957, Threshold calculated is 3561. Anomaly category:Unusual Activity -File Activity Count (Based on User)	Details
onlinedemo	S-1-5-21-1139786260-1848971893-3725018336-1001	log360.com	6-7 AM	Feb 17,2021 06:53:01 AM	3300	5565	Unusual Activity - File Activity Count (Based on User)	5565+ number of File Activity was done by onlinedemo within 6-7 AM. Usual average is 3300, Threshold calculated is 5565. Anomaly category:Unusual Activity -File Activity Count (Based on User)	Details
onlinedemo	S-1-5-21-1139786260-	log360.com							

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。



Actions	Workflow Name	Description	Associated Alert Profiles	Workflow History
  	Block USB	This workflow blocks the USB port on a potential...	0	View History
  	Com alrl one devi run pro noti dayfd - Test.bat		1	View History
  	Disable Computer	This workflow disables a potentially compromised...	0	View History
  	Kill Process	This workflow kills a process on a potentially c...	0	View History
  	Log Off and Disable User	This workflow logs off and disables a potentiall...	0	View History
  	Ping Device		0	View History
  	Popup Alert	This workflow displays a popup alert on the affe...	0	View History
  	Stop Service	This workflow stops a service on a potentially c...	0	View History



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。



ALIEN VAULT

bluechip

威脅情資整合 - 料敵機先

2016-10-16 00:00 2016-10-16 16:35

Alert Profiles [List] + Add Alert Profile Export to : Showing 1 - 50 of 1965 > | 50

Time Generated	Host	Severity	Message
Oct 16, 2016 14:13:59	10.0.0.10	High	Malicious IP found - 222.186.56.42
Oct 16, 2016 14:13:57	10.0.0.10	High	Malicious IP found - 222.186.56.42
Oct 16, 2016 14:13:45	10.0.0.10	High	Malicious IP found - 222.186.56.42
Oct 16, 2016 14:13:45	10.0.0.10	High	Malicious IP found - 222.186.56.42
Oct 16, 2016 14:13:42	10.0.0.10	High	Malicious IP found - 222.186.56.42
Oct 16, 2016 14:13:38	10.0.0.10	High	Malicious IP found - 222.186.56.42
Oct 16, 2016 14:13:34	10.0.0.10	High	Malicious IP found - 222.186.56.42
Oct 16, 2016 14:13:32	10.0.0.10	High	Malicious IP found - 222.186.56.42
Oct 16, 2016 14:13:30	10.0.0.10	High	Malicious IP found - 222.186.56.42
Oct 16, 2016 14:13:30	10.0.0.10	High	Malicious IP found - 222.186.56.42
Oct 16, 2016 14:13:23	10.0.0.10	High	Malicious IP

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

Advanced Threat Analytics ×

Select Threat Source


Info **Geo Info**

 **109.73.66.94**
High Risk

0  100
Reputation Score = 5

Domain name : 109.73.66.94
Domain age : 24
Flagged as malicious on : 2015-11-20 02:02:00
Last occurrence on threat list : 2019-08-18 15:01:41
No. of times it occurred on threat list : 3
Category : Proxy

[Whitelist this source ?](#)

 **Recommendation** : Block IP/URL

Ok

A person in a light blue shirt is sitting at a white desk, working on a laptop. The scene is dimly lit, with the person's face partially visible in profile. The background is a blurred office environment.

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 — 下載20次, 2~3PM — 下載50次, 5~6AM — 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

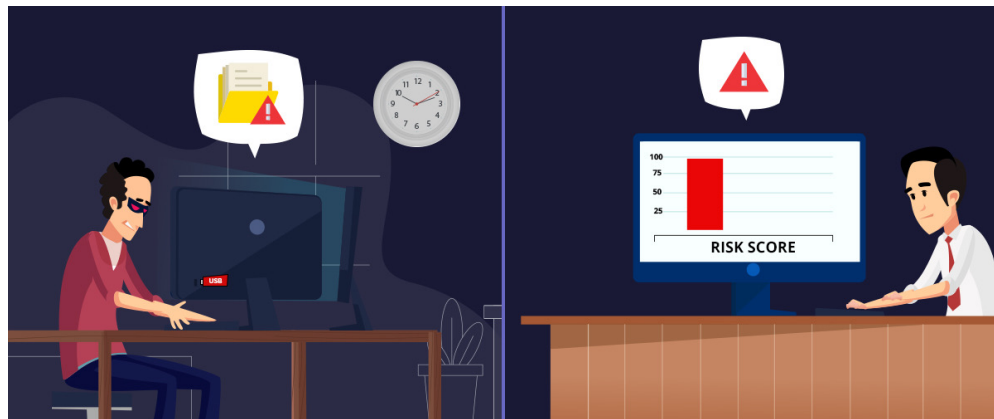


NAT / IT系統管理員

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

The screenshot displays the Log360 user behavior analysis interface. The main dashboard shows a user profile for 'user2' with a risk score of 55. A detailed view of 'user2' is open, showing a 'Card Based Peak Risk Score' and a list of anomalies.

Overall Anomalies: 441

User Risk Score:

User	Last Update	Risk Score
user1	2019-Feb-15 16:29:59	56
user2	2019-Feb-17 08:29:59	55
administrator	2019-Feb-16 16:29:59	51
sa1	2019-Feb-15 16:29:54	47
sa2		

Card Based Peak Risk Score:

Category	Last Update	Score
Insider Threats	2019-Feb-16 18:59:58	67
Data Exfiltration	2019-Feb-16 18:59:59	22
Compromised Accounts	2019-Feb-17 18:30:00	66
Logon Anomalies		0

Peak Risk Score (55) - user2:

Time	Event	Confidence Level
2019-Feb-17	User: 192.168.2.2\user2 Obtained: 153 events Threshold: 16 events	100
08:29:49 2019-Feb-17	Host Registry Accessed Multiple Times By User User: 192.168.2.2\user2 Obtained: 153 events Threshold: 16 events	100
08:29:49 2019-Feb-17	Host Registry Access Failed Multiple Times For User User: 192.168.2.2\user2 Obtained: 153 events Threshold: 16 events	100
08:29:48 2019-Feb-17	Multiple Software Installed By User User: 192.168.2.2\user2 Obtained: 153 events Threshold: 16 events	100

Additional Information:

- Domain/Host/Source: 192.168.2.2
- Average Risk Score: 55
- Peak Risk Score: 55
- Overall Risk Score: 55

Navigation: All Anomalies | Hide from Dashboard

View Details: 55

Timeline: 2019 -> 2020

Text: 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 — 下載20次, 2~3PM — 下載50次, 5~6AM — 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

The screenshot shows the Log360 Compliance dashboard. The top navigation bar includes 'Dashboard', 'Reports', 'Compliance', 'Search', 'Correlation', 'Alerts', 'Settings', 'LogMe', and 'Support'. A 'Download' button is visible in the top right. The left sidebar lists various compliance frameworks: FISMA, PCI-DSS, SOX, HIPAA, GLBA, ISO 27001:2013, GPG, GDPR (highlighted), and ISLP. The main content area is titled 'GDPR' and includes a 'Comprehensive Audit Reports' link. Below this, there are sections for 'Windows Logons' and 'Terminal Service Session'. The 'Windows Logons' section lists events such as 'Windows Successful User Logons', 'Windows UnSuccessful Network L...', 'Windows Successful Network Log...', 'Windows Successful User Logoff...', 'Windows Successful Network Log...', and 'Windows UnSuccessful User Logo...'. The 'Terminal Service Session' section lists 'Terminal Server Connected' and 'Terminal Server Disconnected'.

SIEM 合規報表

The screenshot shows the Log360 Active Directory compliance reports. The top navigation bar includes 'Active Directory' and 'Azure AD'. The left sidebar lists 'User Logon Reports' with sub-items: 'Logon Failures NEW', 'Logon Failures based on users', 'Failures due to Bad Password', and 'Users First and Last Logon By Computers'. The main content area is titled 'User Logon Activ' and includes a 'Folder Permission Changes' link. Below this, there are sections for 'User Logon Activ' and 'User Attribute New and Old Value'. The 'User Logon Activ' section lists events such as 'Member Server Logon Activity' and 'Failed attempt to Read File'. The 'User Attribute New and Old Value' section lists 'User's Last Logon', 'Files Modified', 'File Read Access', and 'User Attribute New and Old Value'.

AD 合規報表

A person in a light blue shirt is sitting at a desk, working on a laptop. The scene is dimly lit, with the person's face partially visible in profile. The background shows a window with blinds. The overall tone is professional and focused.

AD稽核

Active Directory Auditing

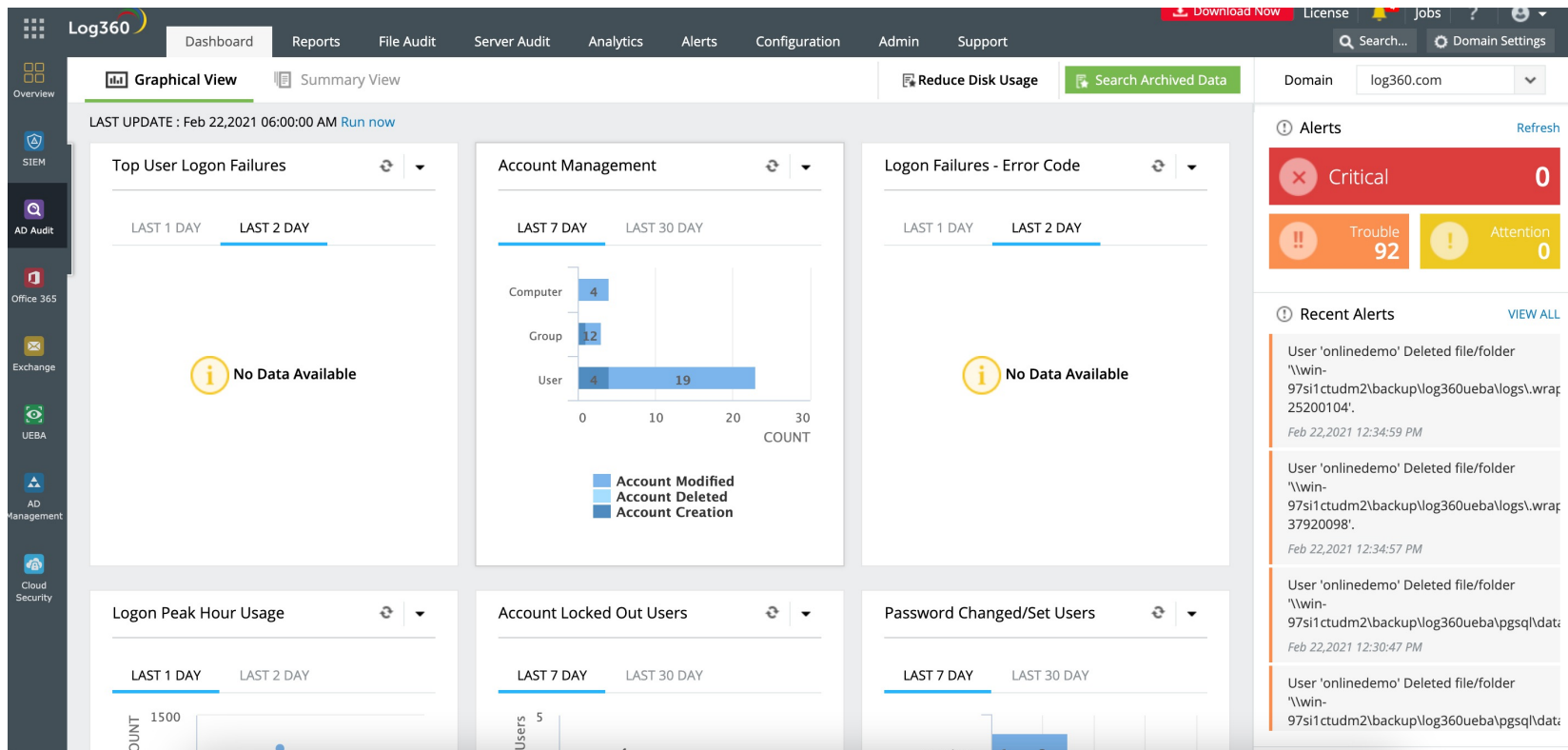
即時稽核 Active Directory 變更

- 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

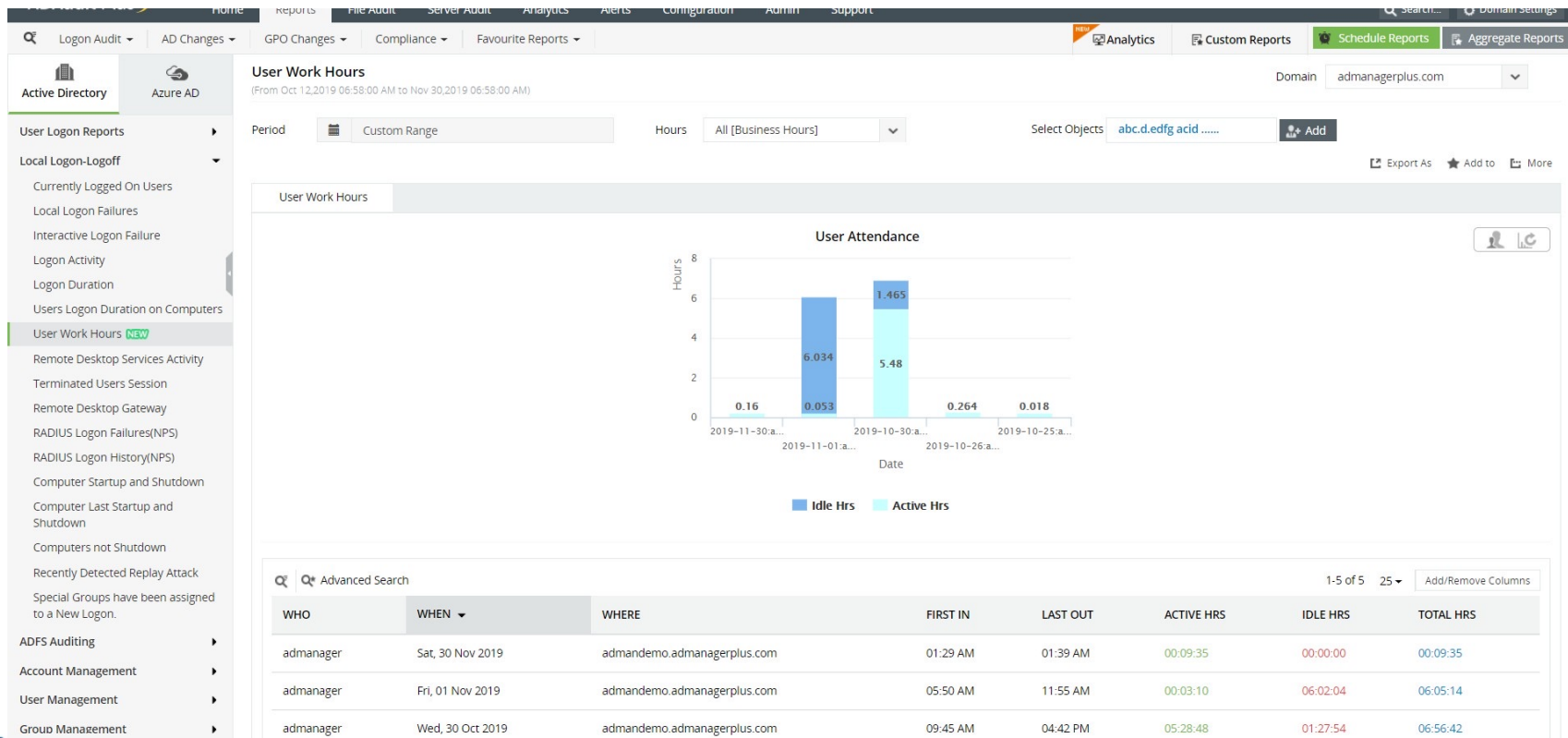
緊密監控 Active Directory 物件

- 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



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

Active Directory > Azure AD > User Logon Reports > User Logon Duration on Computers

Domain: admanagerplus.com

Period: Last 24 Hours | Hours: All [Business Hours] | Select Objects: All

DOMAIN	USER NAME	CLIENT IP ADDRESS	CLIENT HOST NAME	LOGON TIME	LOGOFF TIME	LOGON DURATION	WORKSTATION NAME	LOGON TYPE
ADMANAGERPLUS	admanager	127.0.0.1	admandemo.admanagerplus.com	Apr 08,2020 09:27:50 AM	Apr 08,2020 19:28:55 PM	0 Days, 10:01:05 Hrs	admandemo.admanagerplus.com	Interactive (logon at keyboard and screen of system)
ADMANAGERPLUS	admanager	127.0.0.1	admandemo.admanagerplus.com	Apr 08,2020 09:27:50 AM	Apr 08,2020 09:28:55 AM	0 Days, 00:01:05 Hrs	admandemo.admanagerplus.com	Interactive (logon at keyboard and screen of system)
ADMANAGERPLUS	admanager	127.0.0.1	admandemo.admanagerplus.com	Apr 08,2020 09:26:27 AM	Apr 08,2020 09:28:55 AM	0 Days, 00:02:28 Hrs	admandemo.admanagerplus.com	Interactive (logon at keyboard and screen of system)
ADMANAGERPLUS	admanager	127.0.0.1	admandemo.admanagerplus.com	Apr 08,2020 09:26:27 AM	-	-	admandemo.admanagerplus.com	Interactive (logon at keyboard and screen of system)
ADMANAGERPLUS	admanager	127.0.0.1	admandemo.admanagerplus.com	Apr 08,2020 09:26:19 AM	-	-	admandemo.admanagerplus.com	Interactive (logon at keyboard and screen of system)

AD稽核管理 - 異常登入資安事件報表

Search Reports [Ctrl+Space] Anomalies Risk Assessment Custom Reports Aggregate Reports

Risk Assessment Reports

- Users connected to most assets
- High Activity Volume Accounts
- Hyper Active Accounts
- Accounts with high % of logon failure
- User's Last Admin Activity
- Dormant Admin Account
- Privileges Utilized by user**
- Privilege Escalation - First time Utilizing a Privilege
- Shared Account Based on Remote Logon

Favourite Reports

Privileges Utilized by user

(From Jan 01,2020 10:31:00 AM to Mar 17,2020 10:31:00 AM)

Domain adapdev

Period Custom Range Hours All [BH1] Select Objects All Add

Export As Add to More

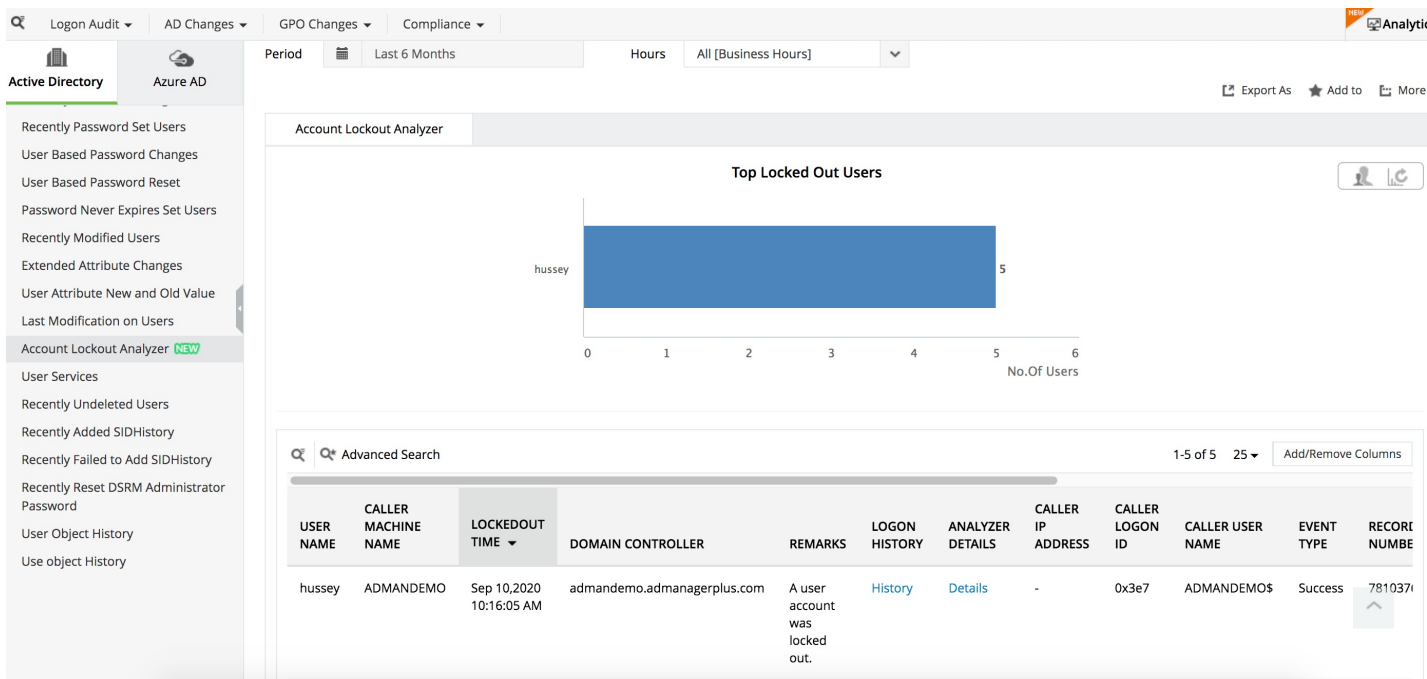
Privileges Utilized by user

Advanced Search 1-25 of 137 25 Add/Remove Columns

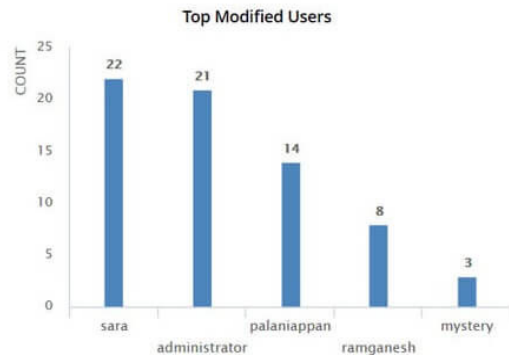
CALLER USER NAME	LAST ACTIVITY TIME	PRIVILEGE UTILIZED	ACTIVITY MESSAGE	ACCOUNT NAME	SID	DOMAIN CONTROLLER	MODIFIED ATTRIBUTES	DOMAIN	CALLER USER DOMAIN
anu	Mar 16,2020 01:04:48 PM	User Modified	User 'abc' was modified by 'ADAPDEV\anu' Modified Properties : User Modified, Values : This is a default account	abc	%(S-1-5-21-1340711753-2541313634-2168098907-1608)	dev-dc1	User Modified	adap.dev.com	ADAPDI
anu	Mar 16,2020 01:04:48 PM	A user account was enabled.	User 'abc' was enabled by 'ADAPDEV\anu'	abc	%(S-1-5-21-1340711753-2541313634-2168098907-1608)	dev-dc1	Account Enabled	ADAPDEV	ADAPDI
anu	Mar 14,2020 09:48:53 PM	Group Attribute Removed	Group 'tes1' was modified by 'ADAPDEV\anu' Modified Properties : member	tes1	%(S-1-5-21-1340711753-2541313634-2168098907-1343)	dev-dc1	Group Modified	adap.dev.com	ADAPDI
anu	Mar 14,2020 09:48:52 PM	A member was removed from a security-enabled global	Member 'CN=t1,OU=ou,OU=poll,DC=adap,DC=dev,DC=com' was removed from Global Security Group 'tes1' by 'ADAPDEV\anu'.	tes1	%(S-1-5-21-1340711753-2541313634-2168098907-1343)	dev-dc1	-	ADAPDEV	ADAPDI

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

A person in a light blue shirt is sitting at a white desk, working on a laptop. The scene is dimly lit, with the person's face partially visible in profile. The background is a blurred office environment.

公有雲日誌管理

A comprehensive cloud log management solution

整合各大雲平台



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	<p>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。</p> <p>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。</p>

A person in a light-colored shirt is sitting at a white desk, using a laptop. The scene is dimly lit, with a window in the background showing a bright outdoor area. The overall tone is professional and focused.

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

Cloud Security Plus Dashboard | Reports | Search | Alerts | Settings | Support | Cloud Account Settings

Account: AWS | Azure | Salesforce | Google

Recently Accessed

Event Details

```
{
  bucketName: "csp-manual-trail-bucket",
  bucketOwner:
    "6ae24bba2a3cc6935b6b278ab435adb779bc1a7ab9ed6e2be420d62d88b8d13c",
  remoteIP: "157.50.145.115",
  totalTime: 28,
  errorCode: "",
  userAgent: "aws-sdk-java/1.11.762 Windows_8.1/6.3 Java_HotSpot(TM)_64-
    Bit_Server_VM/25.51-b03 java/1.8.0_51 groovy/2.0.1
    vendor/Oracle_Corporation",
  requestURI: "GET /AWS_MANUAL/AWSLogs/538582113313/CloudTrail/cn-north-
    1/2020/08/26/538582113313_CloudTrail_cn-north-
    1_20200826T1425Z_XkBbdUqVEa06TvFC.json.gz HTTP/1.1",
  bytesSent: 1101,
  turnAroundTime: 28,
  requestor: "arn:aws-cn:iam::538582113313:user/csp-test-user",
  AccessTime: "26/Aug/2020:14:26:18 +0000",
  referer: "-",
  requestID: "FB80BC5AF6FC7FBA",
  objectSize: 1101,
  eventName: "REST.GET.OBJECT",
  key: "AWS_MANUAL/AWSLogs/538582113313/CloudTrail/cn-north-
    1/2020/08/26/538582113313_CloudTrail_cn-north-
    1_20200826T1425Z_XkBbdUqVEa06TvFC.json.gz",
  HTTPStatus: 200
}
```

1-25 of 1494

Bucket Name	Details
06TvFC.json.gz HTTP/1.1	csp-manual-trail-bucket View
4ssXSS.json.gz HTTP/1.1	csp-manual-trail-bucket View
uv3sy.json.gz HTTP/1.1	csp-manual-trail-bucket View
XnvEw.json.gz HTTP/1.1	csp-manual-trail-bucket View
dJjDn8G.json.gz HTTP/1.1	csp-manual-trail-bucket View
QvT1wR.json.gz HTTP/1.1	csp-manual-trail-bucket View
jXLi2.json.gz HTTP/1.1	csp-manual-trail-bucket View
TDO7Cy.json.gz HTTP/1.1	csp-manual-trail-bucket View

OK

網站檔案被動了!?

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

AWS **AZURE** Salesforce Google

★ Favourite

- Activity by Users
- Permission Changes
- Network Security Groups
 - Rule Changes for Network Security Groups
 - Network Security Group Permission Changes
 - Subnet Changes for Network Security Groups
 - Network Security Groups Created
 - Network Security Groups Deleted
 - Network Security Network Interface Changes
- Virtual Networks
- Application Gateways
- DNS
- Traffic Manager
- Public IP Address

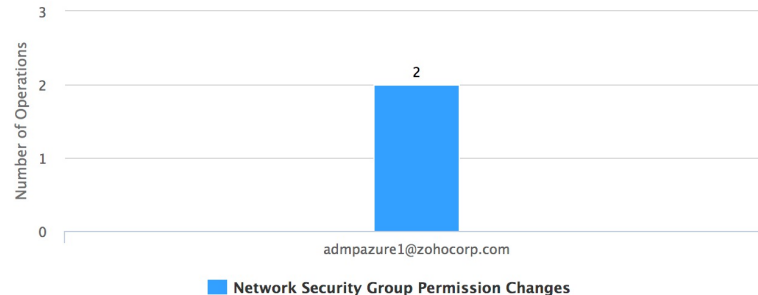
Network Security Group Permission Changes

Account: AZURE

Period: 09-01-2020 - 09-30-2020

Export As More

Top Activity Based on User



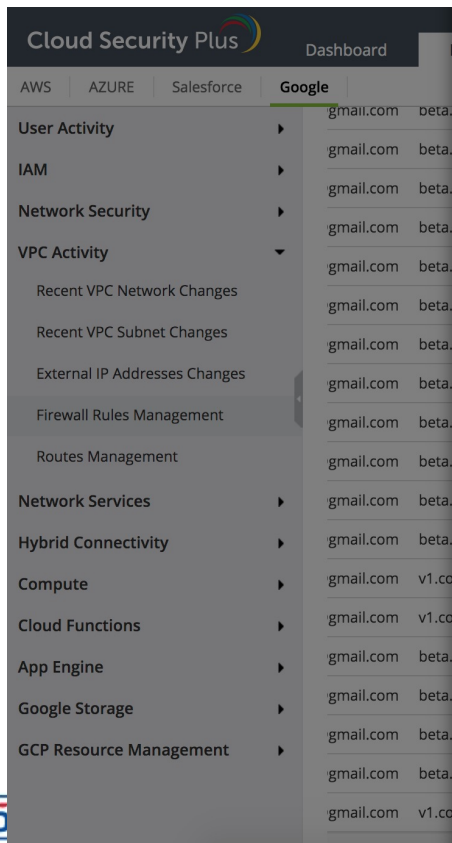
Resource ID	Resource Group Name	Caller	Event Time Stamp	Status	Status Code	Details
delete	1	admpazure1@zohocorp.com	09-10-2020 17:08:12	Succeeded	OK	View
delete	1	admpazure1@zohocorp.com	09-10-2020 17:07:23	Succeeded	Created	View

安全群組權限被改了!?

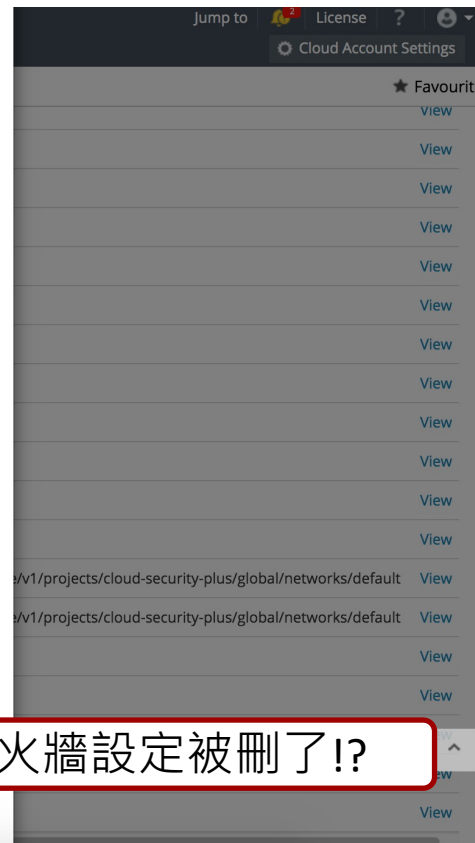
目前還在進化中

- 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?

Figure 1. Magic Quadrant for Security Information and Event Management

連續四屆入圍 Gartner Magic Quadrant for Security Information and Event Management (2016-2018/2020)

#2019並無出刊



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

ManageEngine
Log360

ManageEngine Log360
Vendor Support

**RANKED
1st**

OF 11 IN SECURITY
INCIDENT AND EVENT
MANAGEMENT

88%
SATISFACTION

Powered By
SoftwareReviews

DEGREE OF SATISFACTION

Delights 
Highly Satisfies 
Almost Satisfies 
Disappoints

78%
CATEGORY
AVERAGE

62%
OF CLIENTS ARE
DELIGHTED

ManageEngine
Log360

ManageEngine Log360
Business Value
Created


**RANKED
1st**

OF 11 IN SECURITY
INCIDENT AND EVENT
MANAGEMENT

84%
SATISFACTION

Powered By
SoftwareReviews

DEGREE OF SATISFACTION

Delights 
Highly Satisfies 
Almost Satisfies 
Disappoints

77%
CATEGORY
AVERAGE

43%
OF CLIENTS ARE
DELIGHTED

選擇 Log360

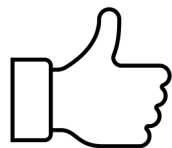
- 五分鐘安裝完畢，簡單管理，支援絕大部分日誌來源
- 結合威脅情資，與使用者行為分析，快速因應資安風險
- 預設合規報表，輕鬆滿足合規需求
- 極具競爭力的價格

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

Introducing 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

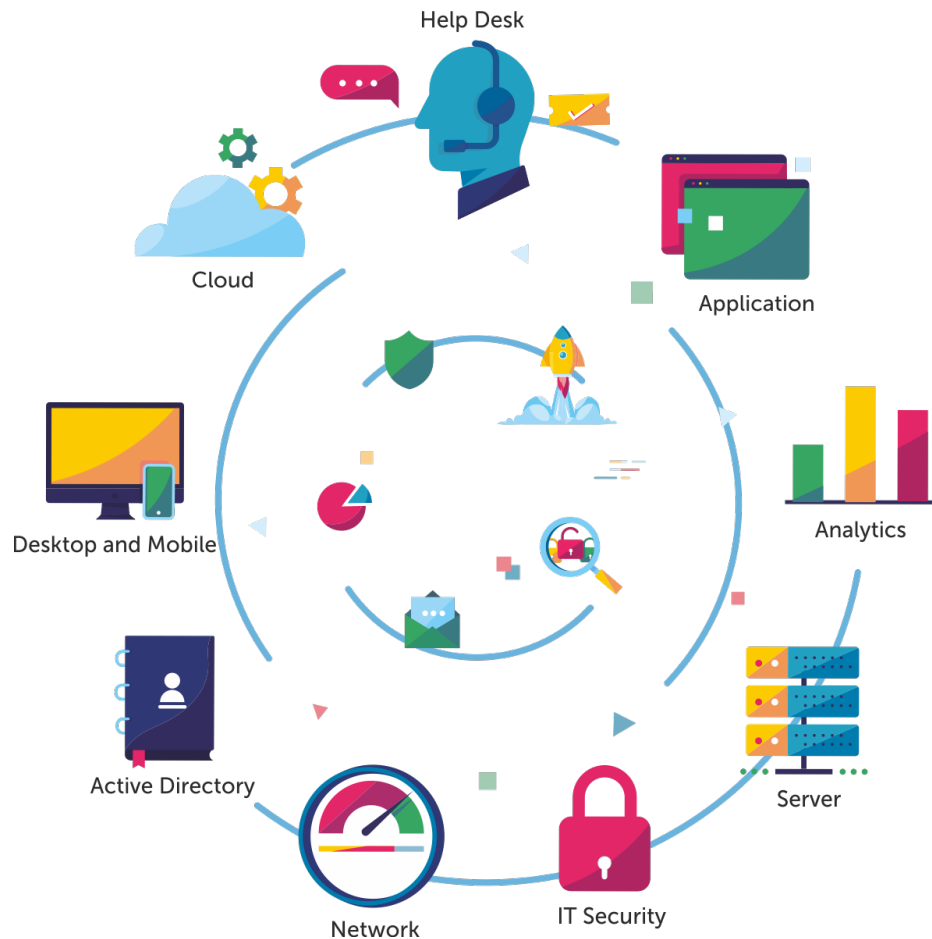
3,000,000+

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
- 大量末端設備
- 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