bluechip infotech

ManageEngine

EventLog Analyzer

SIEM 日誌與資安事件分析管理系統

藍籌科技
張慶振
Kerry Chang

Helping your business grow

20 YEARS 2020

Celebrating 20 Years with Bluechip

PLATINUM SPONSORS

acer CyberPower LogMeIn SOPHOS

GOLD SPONSORS

EATON hp

bluechip 與您的企業一起成長

- 總部位於澳洲雪梨，與其他據點
  - 墨爾本
  - 布里斯本
  - 阿得雷德
  - 伯斯
  - 台北
- 超過101名員工，提供您最佳服務
- 2020上半年營收突破14億台幣(71M AUD)

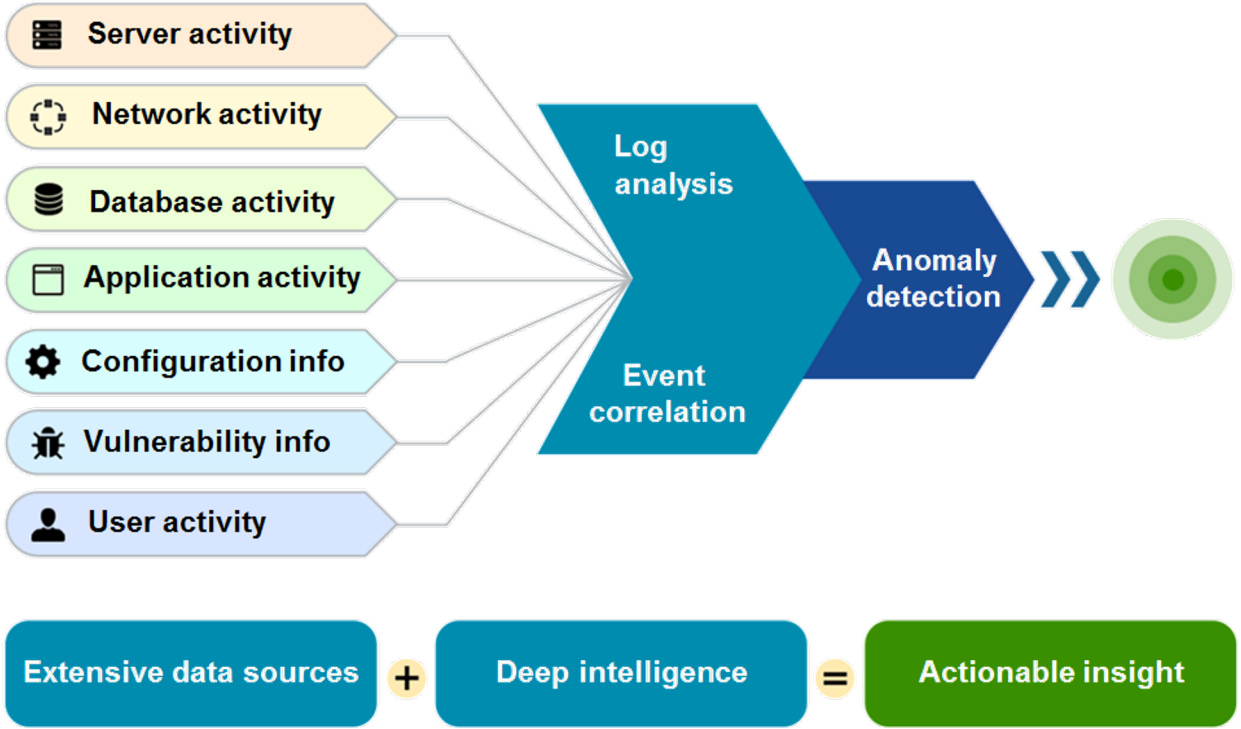
IT管理，與你一起

Helping your business grow

Eventlog Analyzer能幫助您什麼？

What can EventLog Analyzer do?

海納百川，即時偵測


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

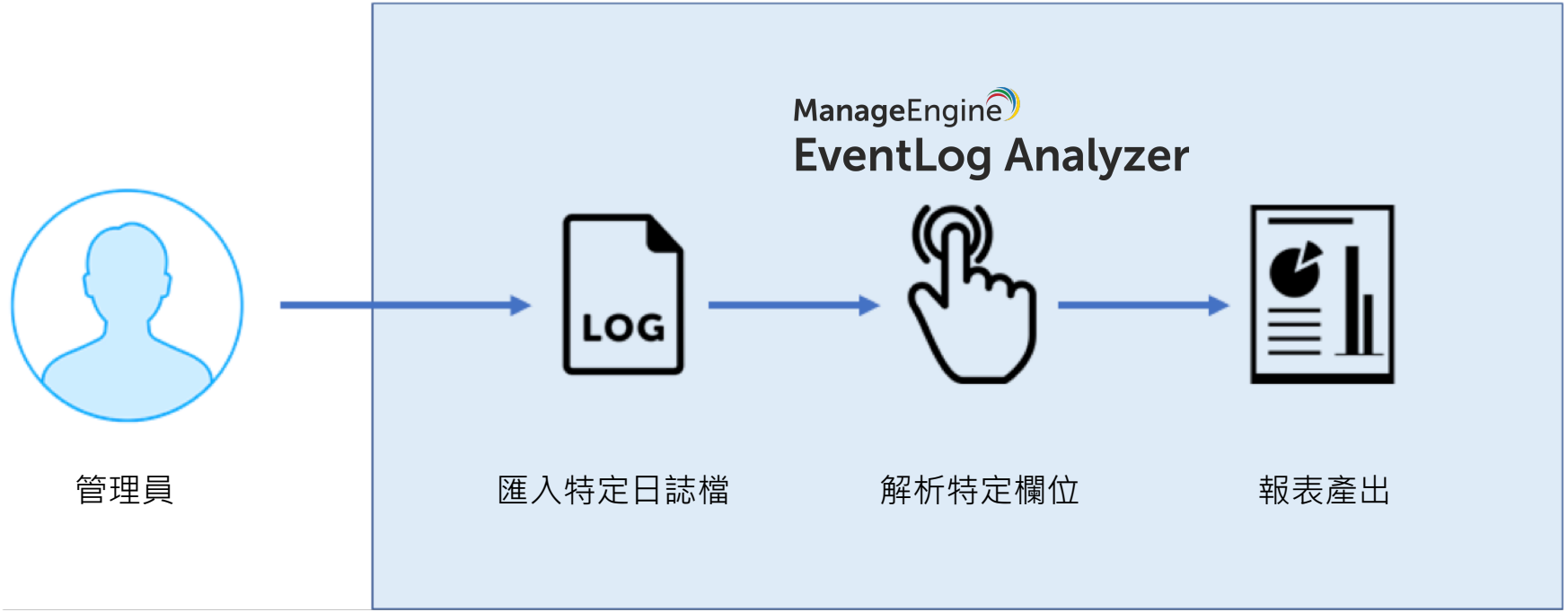
功能介紹

- 日誌管理
  - 收集、分析、統整相關性、備存
- 全面性稽核
  - 網路設備、應用程式
- 智慧型威脅情資
  - 情資告警、事件管理
- 整合合規管理系統

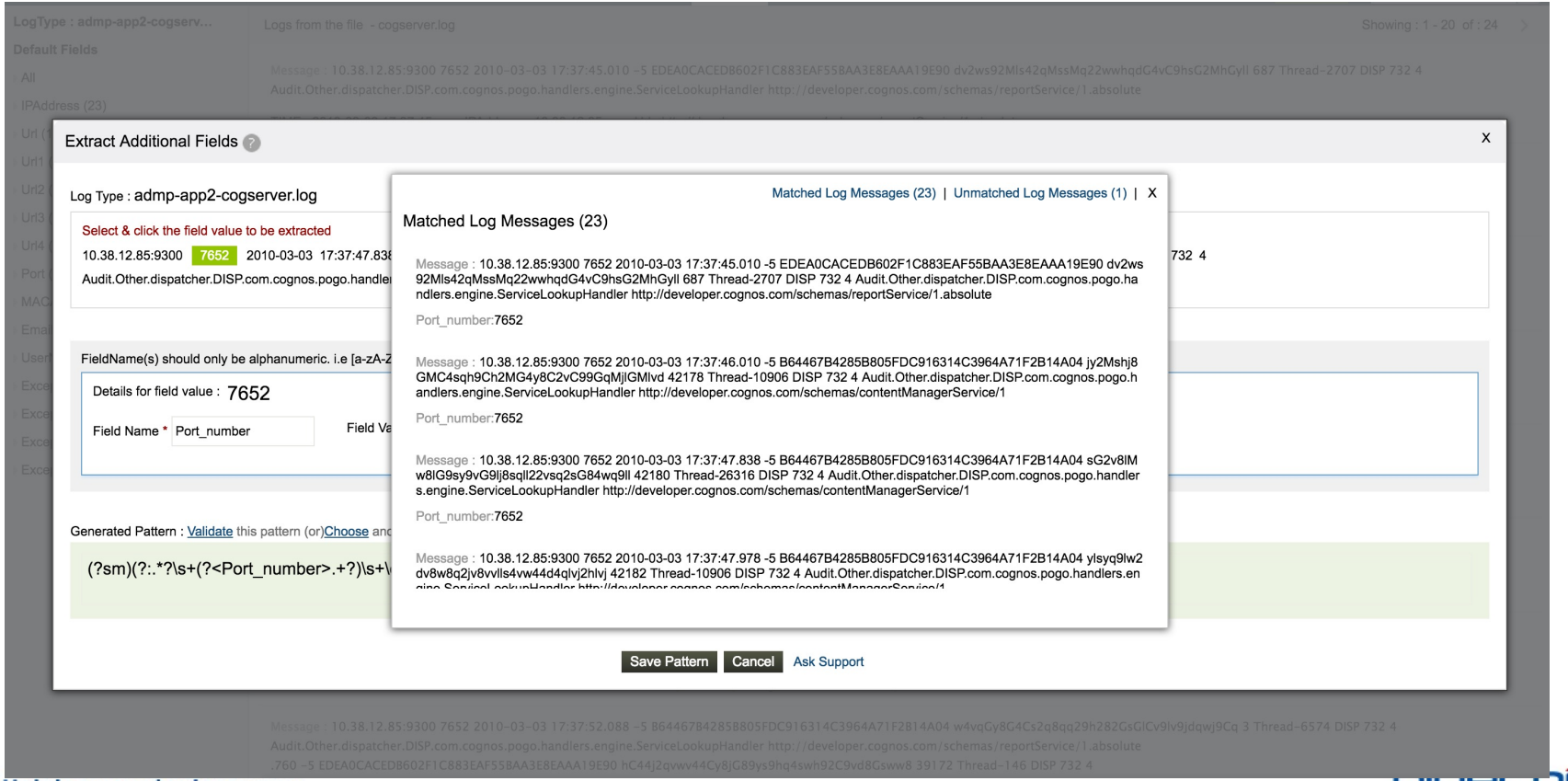
日誌管理

Log Management

日誌收集 - 解析特定日誌


ManageEngine
EventLog Analyzer
LOG
管理員
匯入特定日誌檔
解析特定欄位
報表產出

日誌收集 - 解析特定日誌


Extract Additional Fields
Log Type : admp-app2-cogserver.log
Select & click the field value to be extracted
10.38.12.85:9300 7652 2010-03-03 17:37:47.838
Audit.Other.dispatcher.DISP.com.cognos.pogo.handler
FieldName(s) should only be alphanumeric. i.e [a-zA-Z
Details for field value : 7652
Field Name * Port_number
Generated Pattern : Validate this pattern (or)Choose
(?sm)(?:.*?\s+(?<Port_number>.+?)\s+
Matched Log Messages (23) | Unmatched Log Messages (1) | X
Matched Log Messages (23)
Message : 10.38.12.85:9300 7652 2010-03-03 17:37:45.010 -5 EDEA0CACEDB602F1C883EAF55BAA3E8EAAA19E90 dv2ws92Mls42qMssMq22wwhqdG4vC9hsG2MhGyll 687 Thread-2707 DISP 732 4 Audit.Other.dispatcher.DISP.com.cognos.pogo.handlers.engine.ServiceLookupHandler http://developer.cognos.com/schemas/reportService/1.absolute
Port_number:7652
Message : 10.38.12.85:9300 7652 2010-03-03 17:37:46.010 -5 B64467B4285B805FDC916314C3964A71F2B14A04 jy2Mshj8GMC4sqh9Ch2MG4y8C2vC99GqMjlGMlvd 42178 Thread-10906 DISP 732 4 Audit.Other.dispatcher.DISP.com.cognos.pogo.handlers.engine.ServiceLookupHandler http://developer.cognos.com/schemas/contentManagerService/1
Port_number:7652
Message : 10.38.12.85:9300 7652 2010-03-03 17:37:47.838 -5 B64467B4285B805FDC916314C3964A71F2B14A04 sG2v8lMw8lG9sy9vG9lj8sqll22vsq2sG84wq9ll 42180 Thread-26316 DISP 732 4 Audit.Other.dispatcher.DISP.com.cognos.pogo.handlers.engine.ServiceLookupHandler http://developer.cognos.com/schemas/contentManagerService/1
Port_number:7652
Message : 10.38.12.85:9300 7652 2010-03-03 17:37:47.978 -5 B64467B4285B805FDC916314C3964A71F2B14A04 ylsyq9lw2dv8w8q2jv8vvlls4vw44d4qlvj2hlvj 42182 Thread-10906 DISP 732 4 Audit.Other.dispatcher.DISP.com.cognos.pogo.handlers.engine.ServiceLookupHandler http://developer.cognos.com/schemas/contentManagerService/1
Save Pattern
Cancel
Ask Support

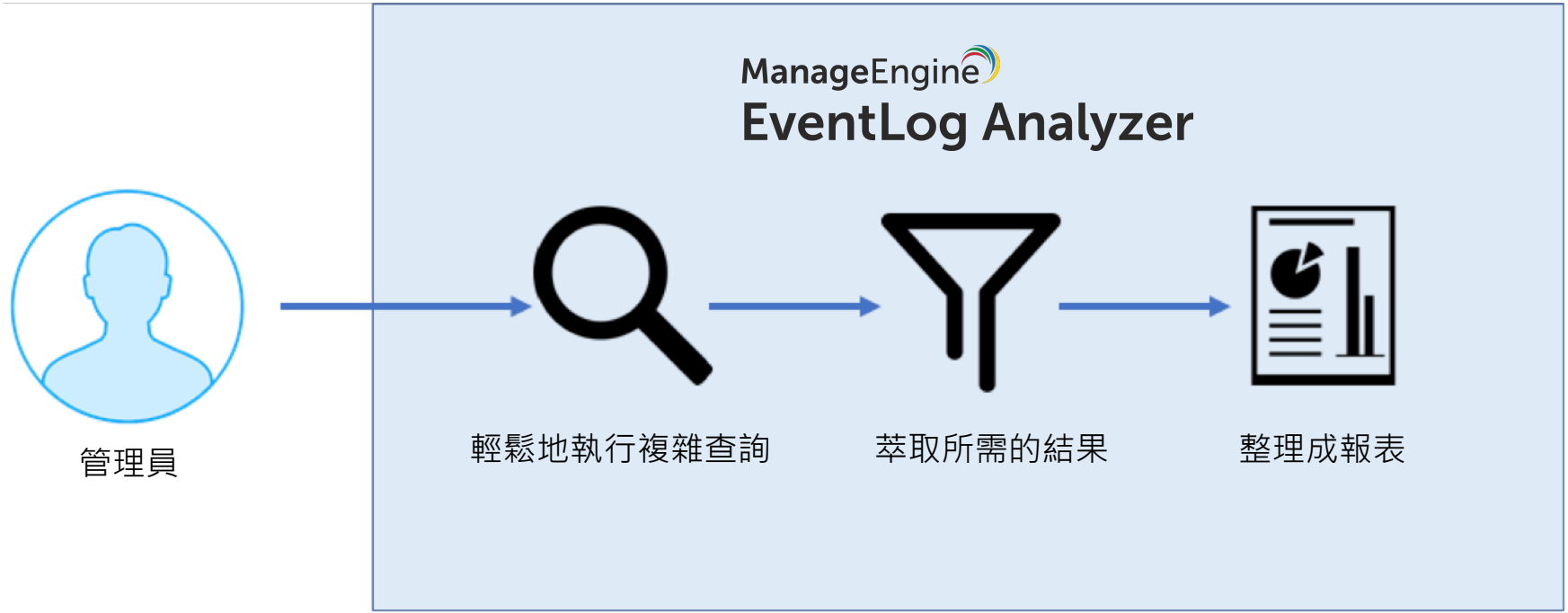
日誌收集 - 支援絕大部分來源

- 支援Agent與無Agent模式
- 支援600種以上日誌來源，包含：
  - 網路設備: routers, switches, IDS/IPS, and firewalls
  - 伺服器: Windows, Linux/Unix, IBM AS400等
  - 資料庫: Oracle and Microsoft SQL
  - 網頁伺服器: Apache and IIS Servers
  - 弱掃與情資解決方案
- 也支援自訂可讀性日誌格式解析

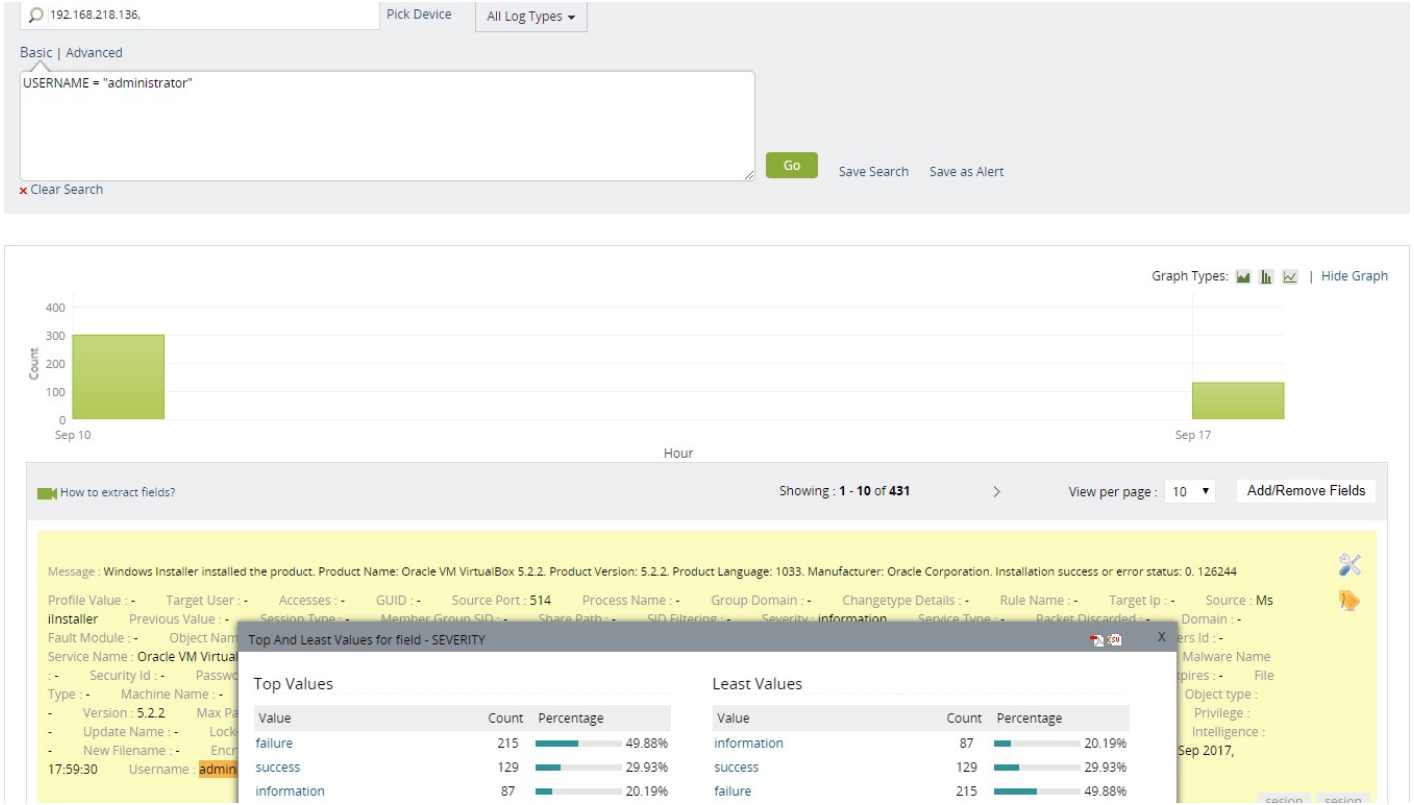
日誌分析

- 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 syslogs
  - 每秒2,000 Windows 事件日誌

日誌分析 - 日誌鑑識


ManageEngine
EventLog Analyzer
管理員
輕鬆地執行複雜查詢
萃取所需的結果
整理成報表

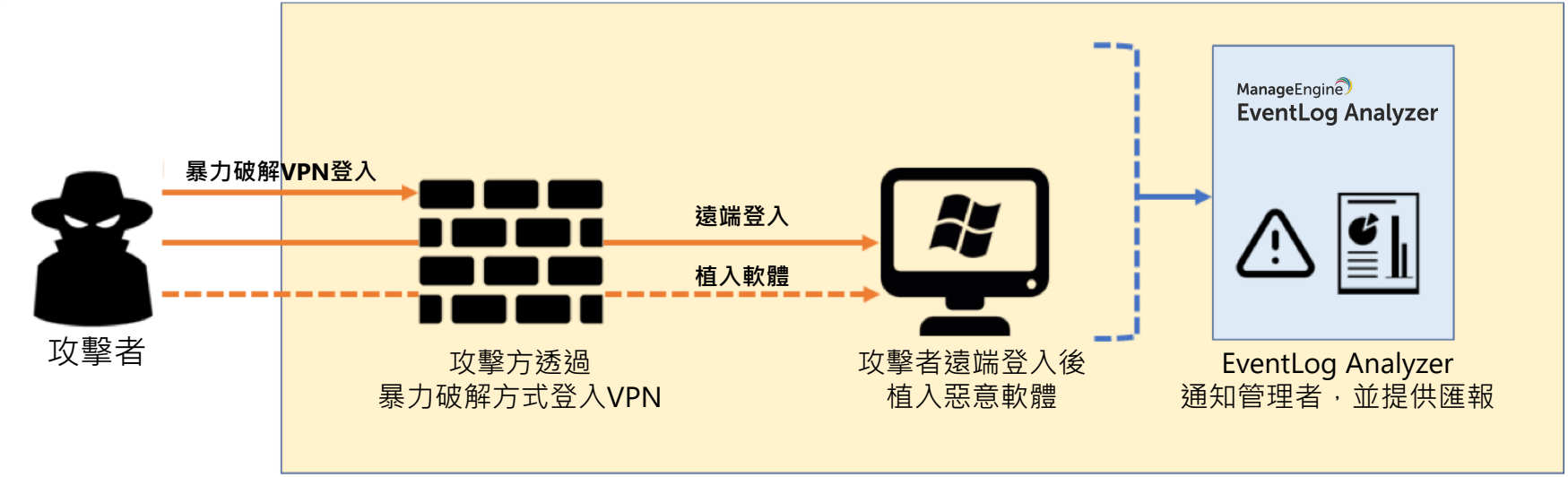
日誌分析 - 日誌萃取


192.168.218.136,
Pick Device
All Log Types
Basic | Advanced
USERNAME = "administrator"
Go
Save Search
Save as Alert
Clear Search
Graph Types:
Hide Graph
400
300
200
100
0
Count
Sep 10
Sep 17
Hour
How to extract fields?
Showing : 1 - 10 of 431
View per page : 10
Add/Remove Fields
Message : Windows Installer installed the product. Product Name: Oracle VM VirtualBox 5.2.2. Product Version: 5.2.2. Product Language: 1033. Manufacturer: Oracle Corporation. Installation success or error status: 0. 126244
Top And Least Values for field - SEVERITY
Top Values
Value Count Percentage
failure 215 49.88%
success 129 29.93%
information 87 20.19%
Least Values
Value Count Percentage
information 87 20.19%
success 129 29.93%
failure 215 49.88%

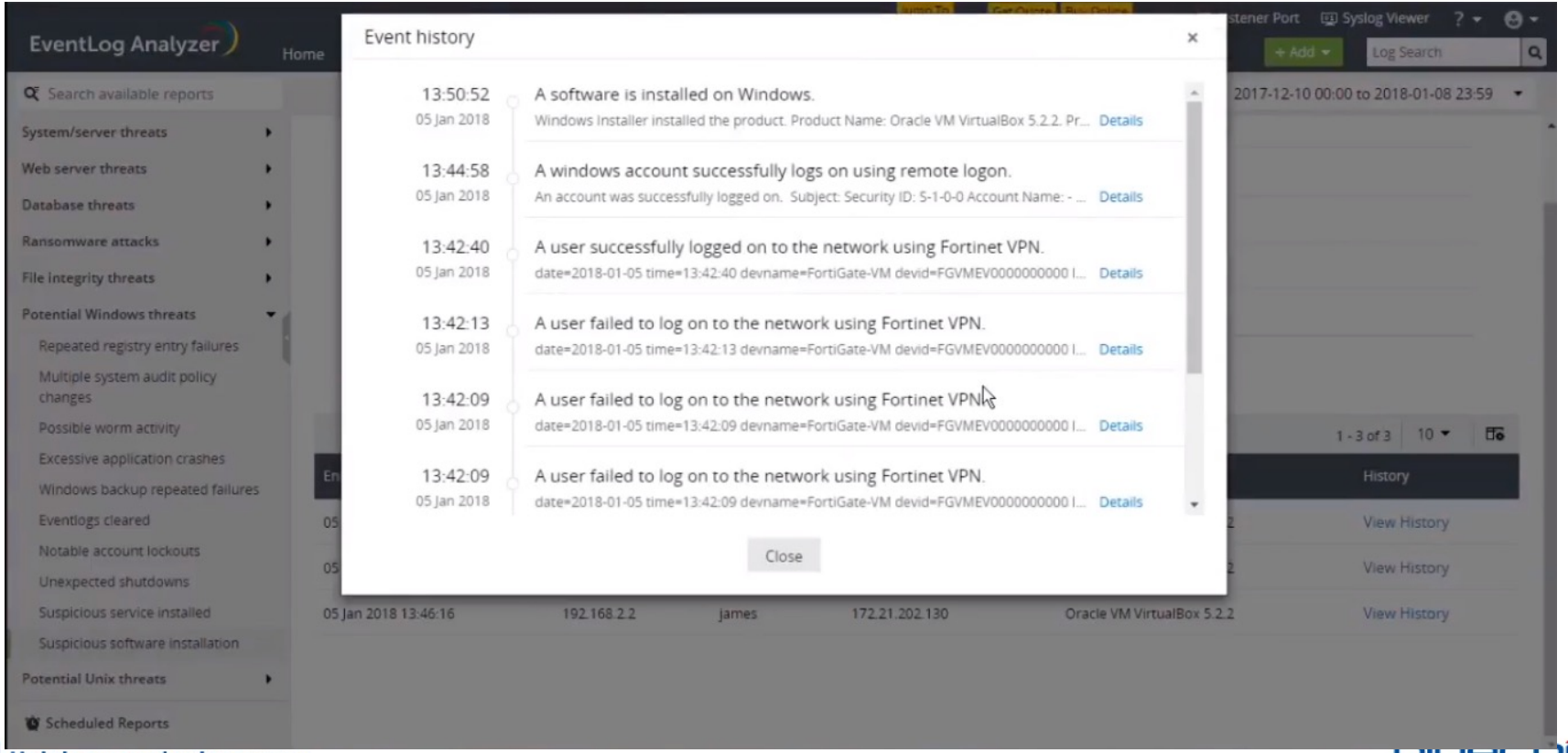
日誌分析 - 關聯性分析

- 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

日誌分析 - 關聯性分析


暴力破解VPN登入
遠端登入
植入軟體
ManageEngine
EventLog Analyzer
攻擊者
攻擊方透過
暴力破解方式登入VPN
攻擊者遠端登入後
植入惡意軟體
EventLog Analyzer
通知管理者，並提供匯報

日誌分析 - 關聯性案例分析



日誌備存

- 將日誌文件加密，以確保日誌資料的安全性，必要時，提供將來進行偵查分析、合規性驗證與內部稽核。
- 預設情況下，每24小時建立一個日誌歸檔文件，包含所有接收到的原始日誌。且將這些文件，以每7天的頻率壓縮一次以節省儲存空間。
- 隨時都可以將文件讀取至EventLog Analyzer資料庫中，並且可以為已存檔的事件資料整理後，產出報表。

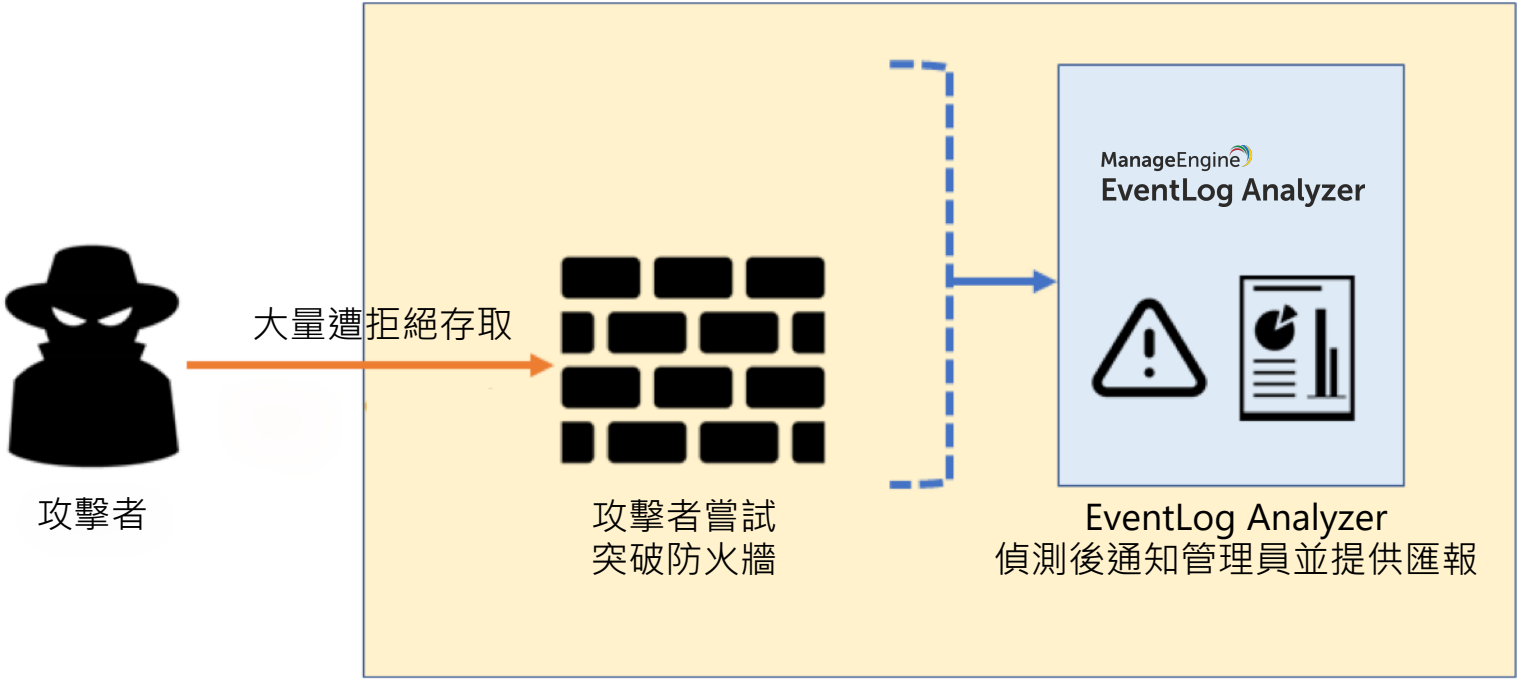
全面性稽核

Comprehensive Auditing

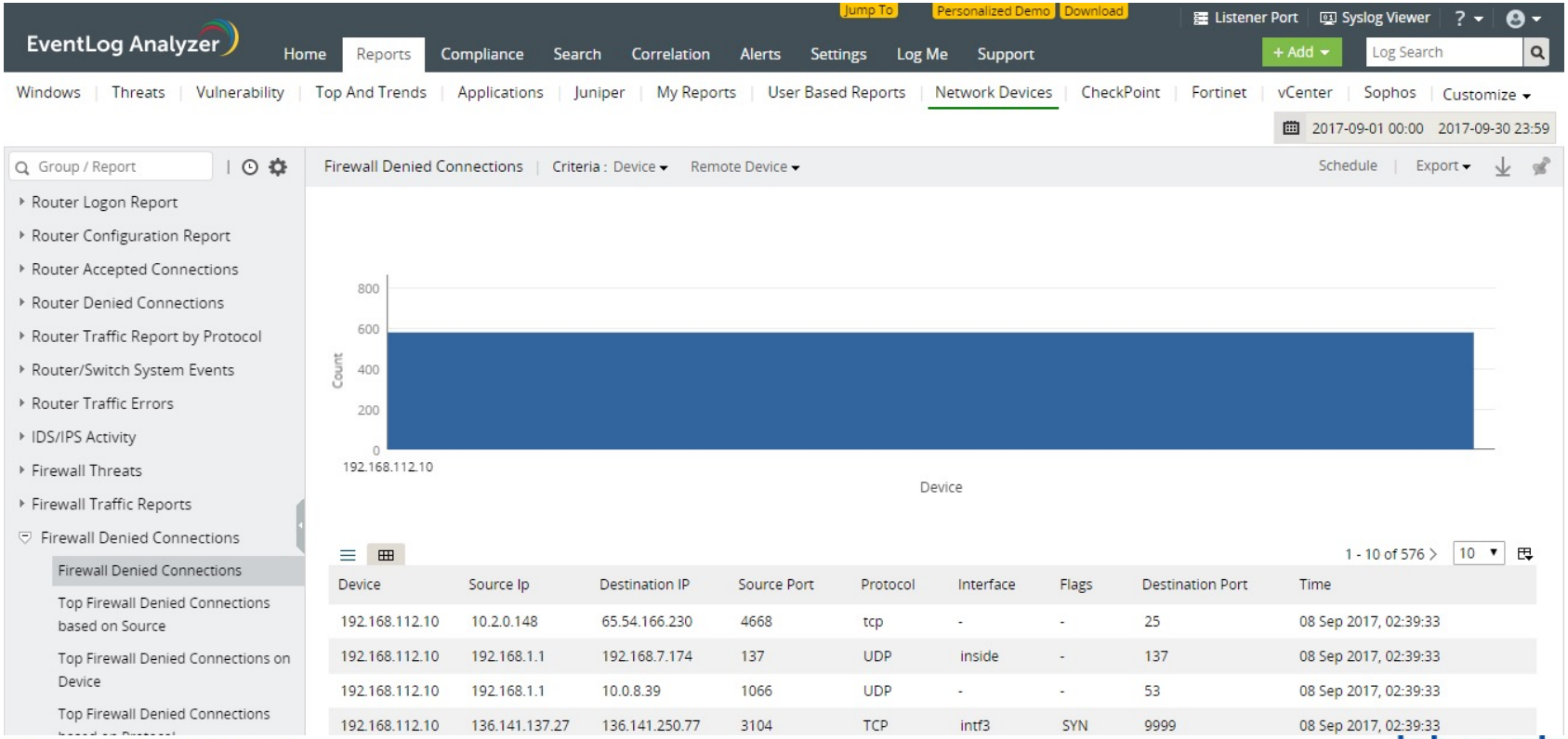
網路設備稽核

- 監控防火牆設定與規則變更
- 監控設備上未經授權身份的存取，與異常權限提升。
- 檢測路由器，交換機，防火牆和IDS / IPS設備上被拒絕的異常連線，威脅和其他資安事件。

網路設備稽核範例 - 防火牆奇襲



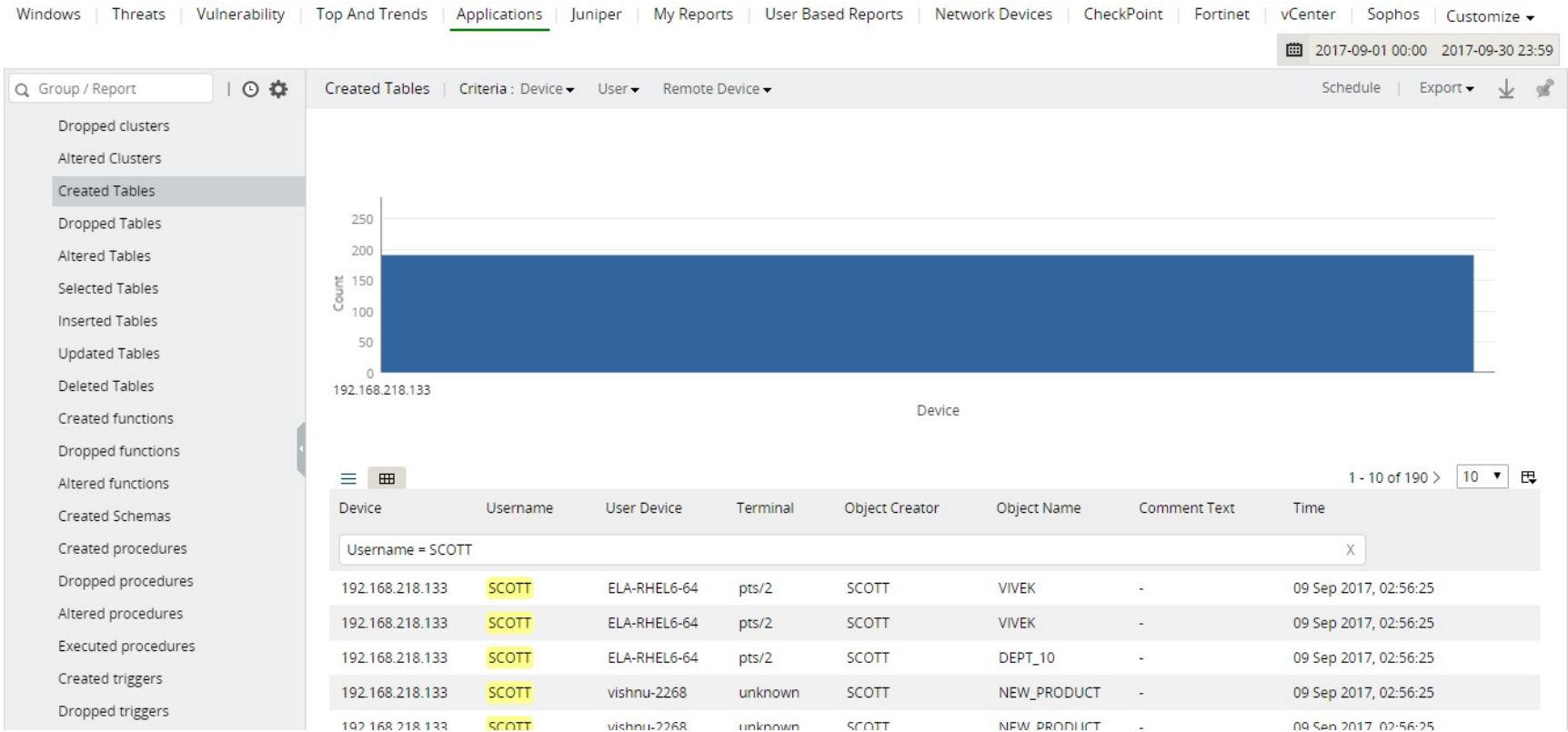
網路設備稽核範例 - 防火牆奇襲



應用程式稽核

- 自動導入應用程式日誌資料
  - 從匯入的日誌中萃取資安報表，並使用可自訂的日誌解析器，分析內部應用程式日誌。
- 保護IIS和Apache Web服務器的安全
  - 即時識別異常活動，例如錯誤事件，暴力破解和伺服器攻擊。
- Microsoft SQL Server和Oracle資料庫稽核：
  - 追蹤使用者操作，DML和DDL查詢，資料庫資料更新，以及伺服器帳戶變動。
- 稽核弱掃和情資解決方案：
  - 透過預測分析，詳細了解最易受攻擊的埠號、主機，病毒感染、資料竊取等潛在的資安風險。

應用程式稽核 - 特定使用者新增資料表

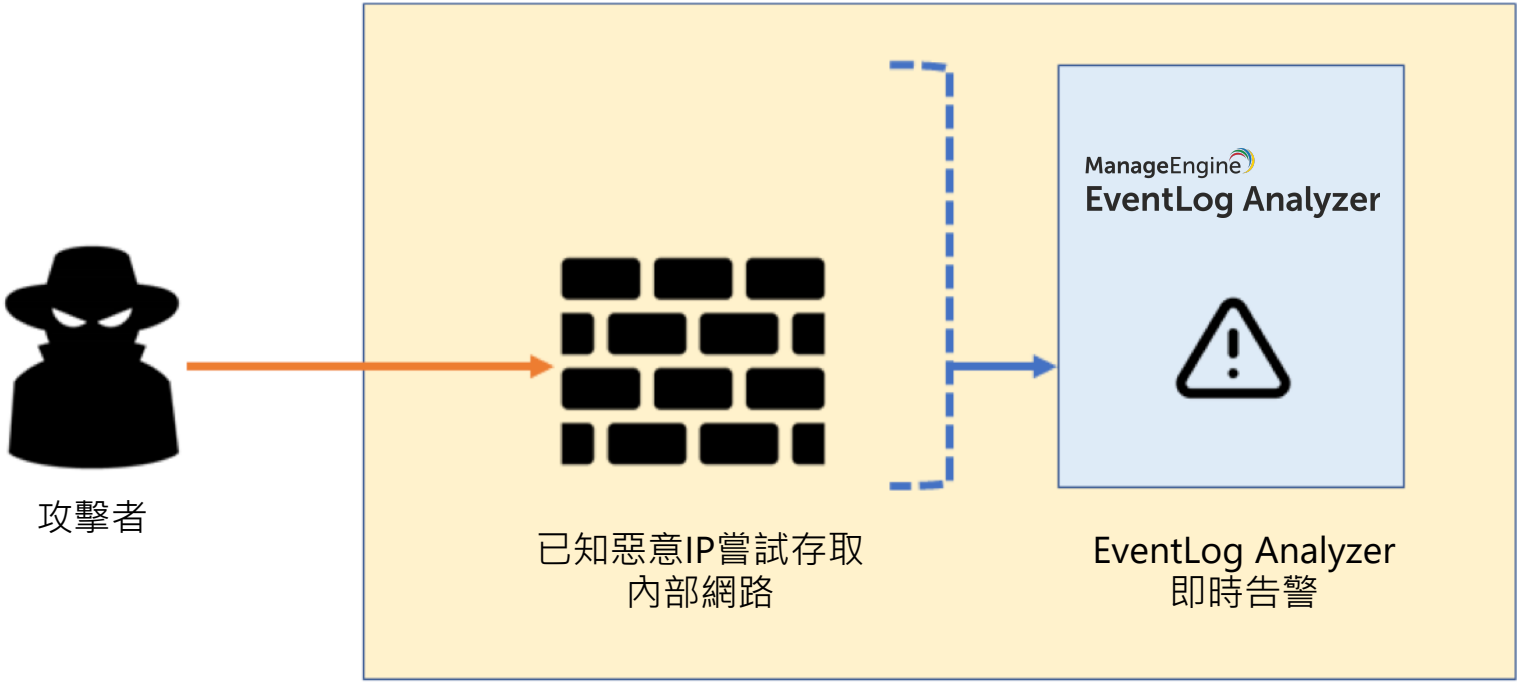



智慧型威脅情資
Threat Intelligence

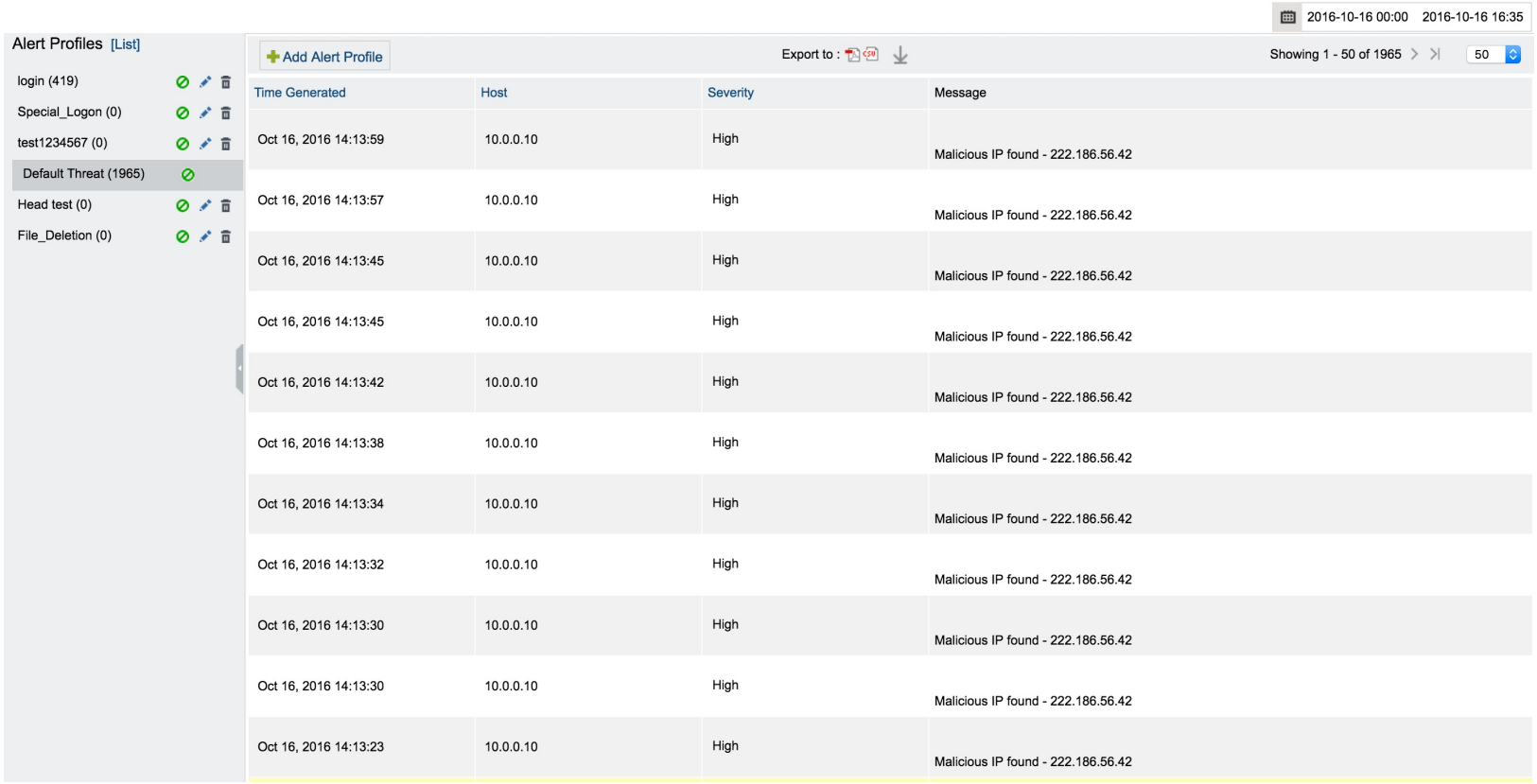
情資威脅告警

- EventLog Analyzer接收多個Open Source(例如AlienVault)和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。

情資威脅告警範例


ManageEngine
EventLog Analyzer
攻擊者
已知惡意IP嘗試存取
內部網路
EventLog Analyzer
即時告警

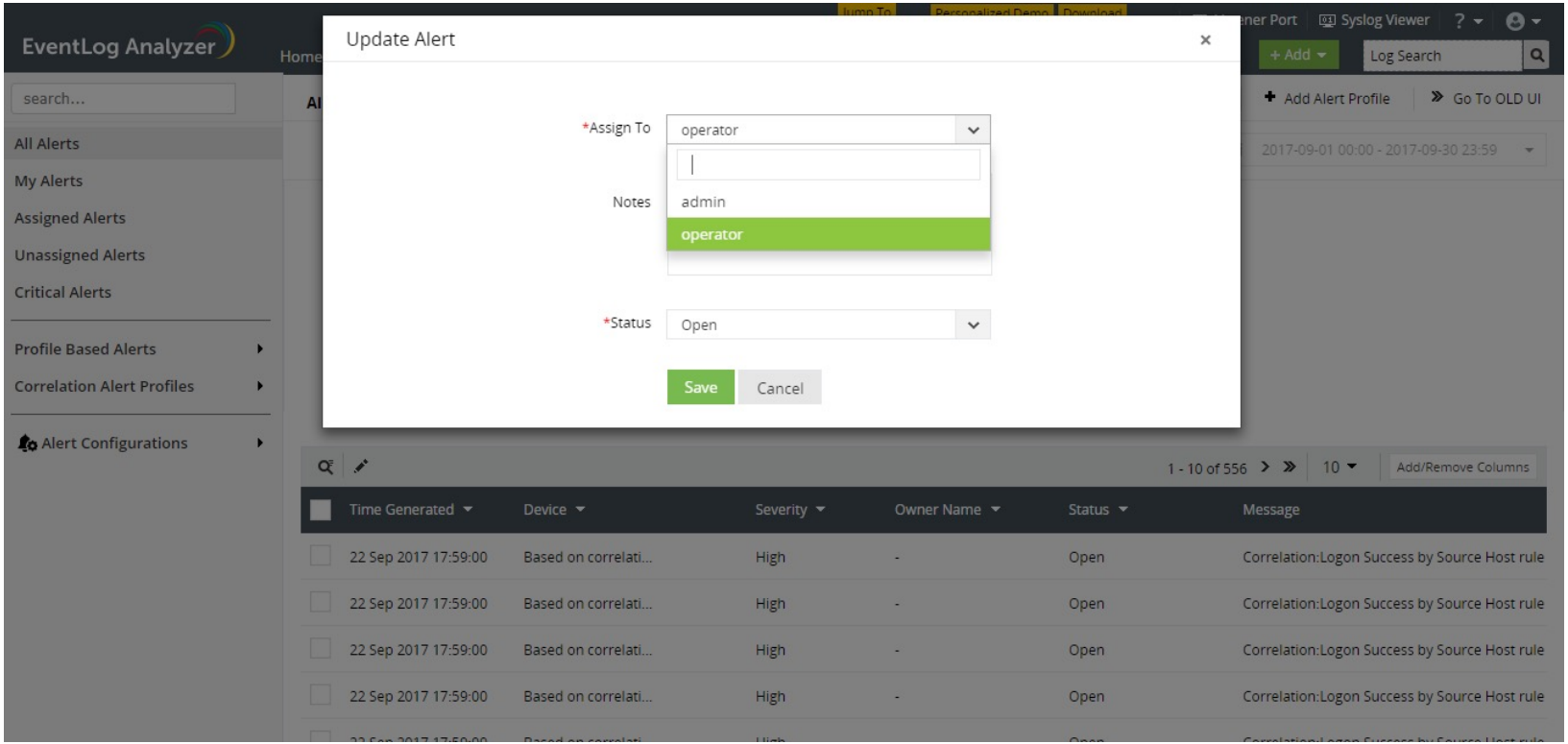
情資威脅告警範例


2016-10-16 00:00 2016-10-16 16:35
Alert Profiles [List]
login (419)
Special_Logon (0)
test1234567 (0)
Default Threat (1965)
Head test (0)
File_Deletion (0)
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 found - 222.186.56.42

事件管理

- 使用內建的事件管理平台，管理資安事件。
- 自動將報修單，分配給各系統之管理員。
- 追蹤事件報修單，使用多個視圖篩選報修等。
- 也可以將事件，轉發到其他事件管理系統。

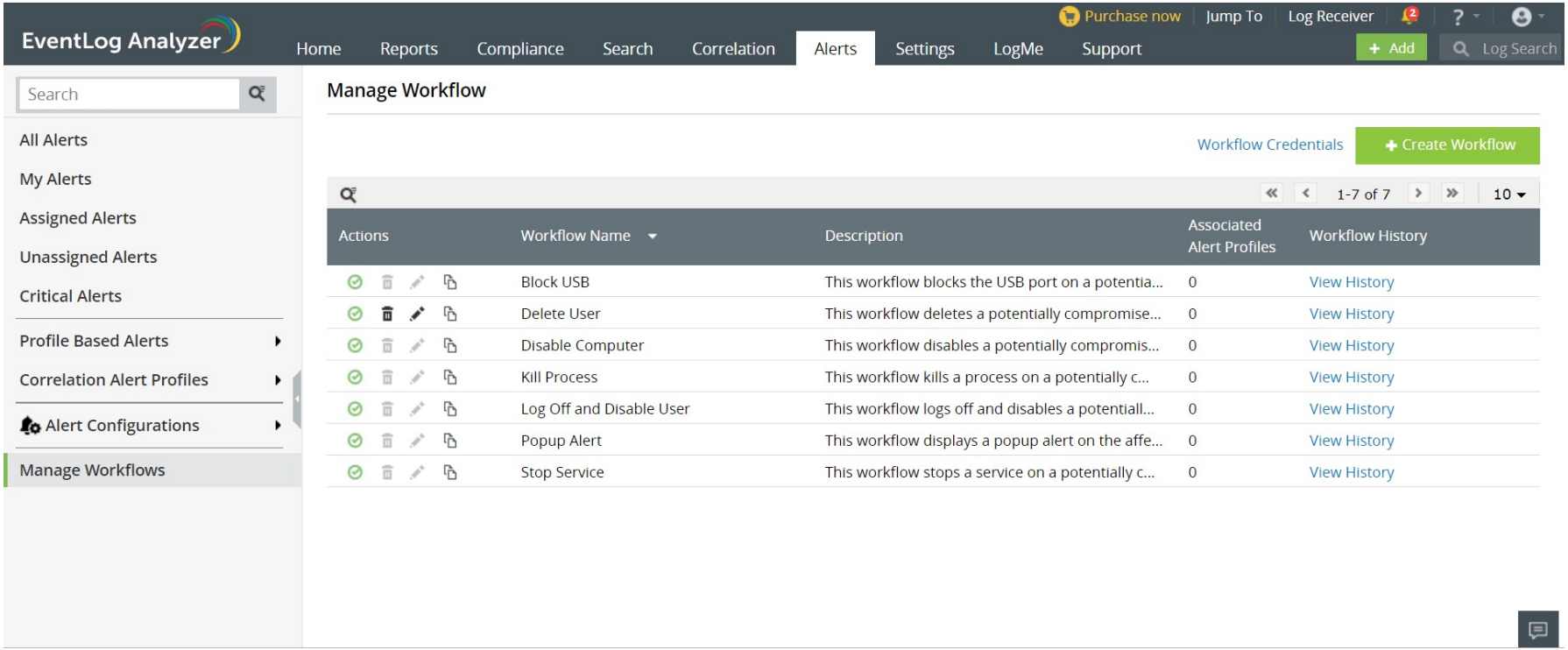
事件管理範例


EventLog Analyzer
Update Alert
*Assign To
operator
admin
operator
Notes
*Status
Open
Save
Cancel
Log Search
Add Alert Profile
Go To OLD UI
All Alerts
My Alerts
Assigned Alerts
Unassigned Alerts
Critical Alerts
Profile Based Alerts
Correlation Alert Profiles
Alert Configurations
Time Generated
Device
Severity
Owner Name
Status
Message
22 Sep 2017 17:59:00
Based on correlati...
High
Open
Correlation:Logon Success by Source Host rule

自動化工作流程

- 通過自動化事件回應管理來遏制攻擊或降低其影響。
- 將預先制定的自動工作流程與告警設定做關聯，達到自動修復檢測到的資安事件。
- 新增和管理事件工作流程，讓這些工作流程在觸發安全告警時自動執行。
- 使用EventLog Analyzer的內建工作流程或根據您的要求，使用靈活的工作流程設定工具來自訂工作流程規則，。

自動化工作流程 - 範例


EventLog Analyzer
Purchase now
Jump To
Log Receiver
Home
Reports
Compliance
Search
Correlation
Alerts
Settings
LogMe
Support
Add
Log Search
Search
All Alerts
My Alerts
Assigned Alerts
Unassigned Alerts
Critical Alerts
Profile Based Alerts
Correlation Alert Profiles
Alert Configurations
Manage Workflows
Manage Workflow
Workflow Credentials
Create Workflow
1-7 of 7
10
Actions
Workflow Name
Description
Associated Alert Profiles
Workflow History
Block USB
This workflow blocks the USB port on a potentia...
0
View History
Delete User
This workflow deletes a potentially compromise...
0
View History
Disable Computer
This workflow disables a potentially compromis...
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
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

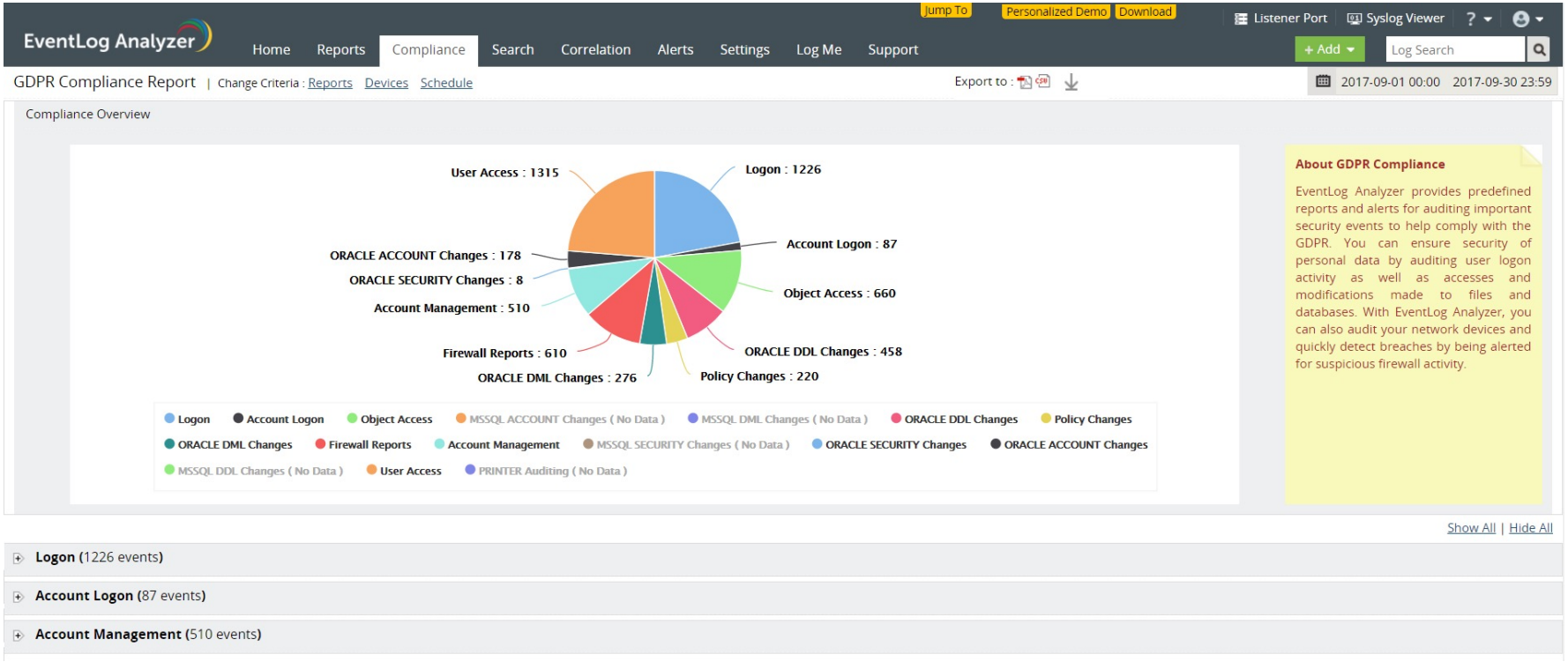
整合合規管理系統

Integrated Compliance Management System

整合合規管理系統

- 產出以下現成合規報告：
  - PCI DSS , GDPR , FISMA , HIPAA , GLBA , SOX , ISO 27001
- 新建或修改現有合規性報告以滿足內部資安策略。
- 強大的搜索功能和安全的日誌歸檔功能，可滿足大多數合規性策略的取證分析和日誌歸檔需求。

整合合規管理系統


EventLog Analyzer
Jump To
Personalized Demo
Download
Listener Port
Syslog Viewer
Home
Reports
Compliance
Search
Correlation
Alerts
Settings
Log Me
Support
+ Add
Log Search
GDPR Compliance Report | Change Criteria : Reports Devices Schedule
Export to :
2017-09-01 00:00 2017-09-30 23:59
Compliance Overview
User Access : 1315
Logon : 1226
ORACLE ACCOUNT Changes : 178
Account Logon : 87
ORACLE SECURITY Changes : 8
Object Access : 660
Account Management : 510
Firewall Reports : 610
ORACLE DDL Changes : 458
ORACLE DML Changes : 276
Policy Changes : 220
Logon
Account Logon
Object Access
MSSQL ACCOUNT Changes (No Data)
MSSQL DML Changes (No Data)
ORACLE DDL Changes
Policy Changes
ORACLE DML Changes
Firewall Reports
Account Management
MSSQL SECURITY Changes (No Data)
ORACLE SECURITY Changes
ORACLE ACCOUNT Changes
MSSQL DDL Changes (No Data)
User Access
PRINTER Auditing (No Data)
About GDPR Compliance
EventLog Analyzer provides predefined reports and alerts for auditing important security events to help comply with the GDPR. You can ensure security of personal data by auditing user logon activity as well as accesses and modifications made to files and databases. With EventLog Analyzer, you can also audit your network devices and quickly detect breaches by being alerted for suspicious firewall activity.
Show All | Hide All
Logon (1226 events)
Account Logon (87 events)
Account Management (510 events)


Why Eventlog Analyzer?
Why not?

選擇 Eventlog Analyzer

- 五分鐘安裝完畢，簡單管理
- 綜觀全場，支援大多數日誌來源
- 無需額外添購加值服務
- 極具競爭力的價格

最小安裝環境

- Processor cores：2
- RAM：4 GB
- Disk Throughput：6 MB/s
- Disk space：300 GB
- Network card capacity：1 Gb/s
- CPU architecture：32/64bit
- Windows 8/10, and Windows Server 2012/2016/2019
- Linux: Red Hat 8.0/8.2/9.0/RHEL, Mandrake/Mandriva, SUSE, Fedora, CentOS, Ubuntu, Debian

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

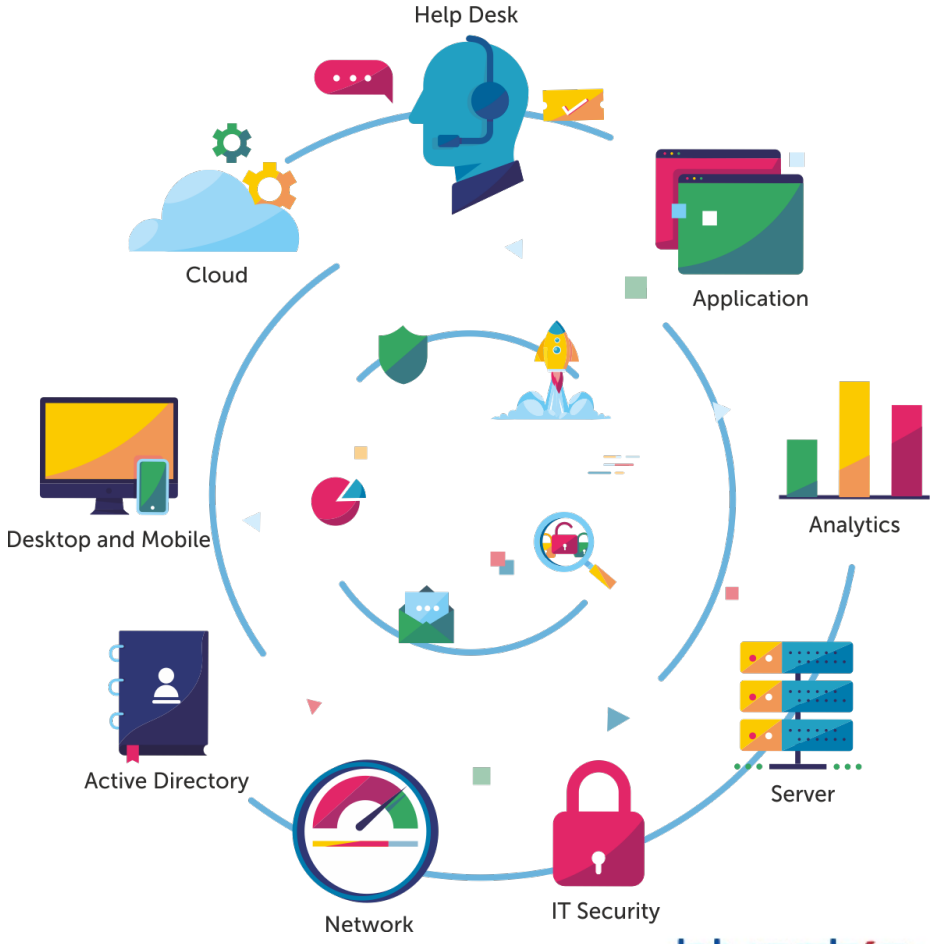
9/10
財富 100 強公司

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




WHO can help?

IT's ManageEngine

找Kerry吧

Email:kerryc@bcit.com.tw

THANK YOU

Any Questions?

Or

Contact Kerry