AlienVault USM - 資訊安全管理平台

以強大的威脅情資庫爲基礎的全方位資安防護

AlienVault USM 是一個部署於本地端網路內的多合一資訊安全管理平台，可將各種資安事件來源集中化管理，並同時進行威脅偵測、事件響應與合規性管理。透過 USM 強大的資訊收集能力，搭配 AlienLabs 傲視全球的威脅情資平台，在眞正的意義上實現主動式防禦體系。

多功能平台滿足資安監控的需求

USM 是多功能的資訊安全管理平台，包含了資產管理、弱點評估、入侵偵測(網路、主機、以及雲端)、事件響應、SIEM、以及日誌管理功能。USM 能夠針對您的網路環境進行資訊收集、威脅分析、威脅驗證和管理威脅訊息，並透過內建的強大威脅情資資料庫，即時提供 IT 管理人員相關情資及相關事件詳細資訊，藉以進行適當的事故處理。

全球最強的資安威脅情資體制

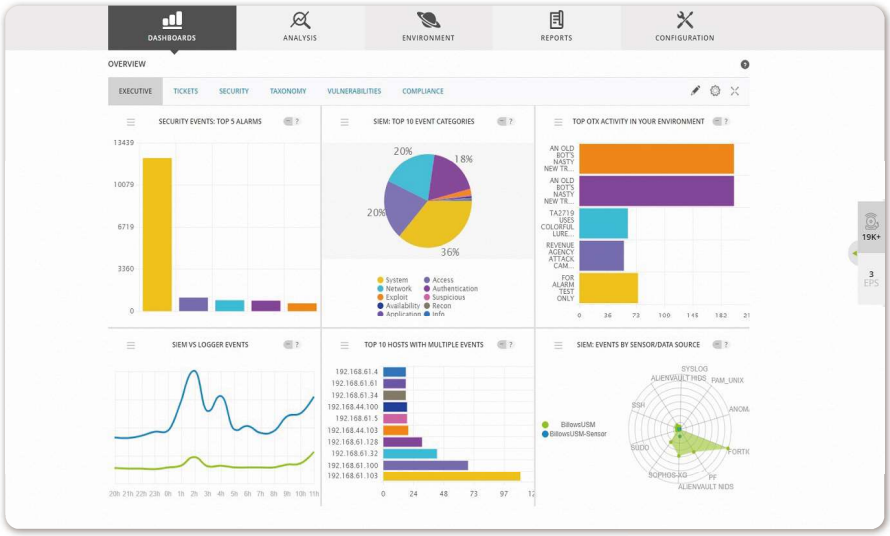
由於情資來源的局限以及更新效率等問題，目前常見的威脅共享或區域聯防體制在實務上仍充斥著許多資安盲點。在主動式防禦的體系下，威脅情資的更新速度將是與駭客互相搏鬥的勝敗關鍵。身爲全球網路安全聯盟成員，AT&T AlienLabs 所提供的威脅情資平台在全球104個國家/地區擁有 100,000 多名參與者，每天貢獻超過 1,900 萬個威脅指標。由 AT&T 所提供的威脅情資，使組織能夠快速接收到最新的網路攻擊與威脅事件，能眞正有效地即時共享威脅情資，並建立完善的聯防體制。

專家團隊全天候產製偵測規則

當採購了 SOC 服務或是 SIEM 之後，若沒有持續更新威脅偵測規則，那麼就如同買了一張破網一樣，永遠會有漏網之魚。AT&T AlienLabs 擁有一支由資深安全專家所組成的團隊，根據最新發生的威脅事件進行即時分析，產製威脅關聯規則以及各種入侵偵測指標，協助您將威脅阻絕於外，是您安全團隊的最佳後盾。

法規遵循的最佳工具

由於網路攻擊事件頻傳，企業爲證明自身資訊防護具有一定的水準，紛紛導入不同的資安遵循框架(NIST CSF、COBIT)以及國際資安標準 / 法規(HIPAA、PCI-DSS、GDPR)。USM 可針對現行國際通行的標準或是企業自定義的安全基準提供相關的稽核報告，也相容於國內資安法框架，同時透過 USM 多樣化的儀表板，能夠讓您輕鬆查看內部安控的狀況，並做出相應調整。



圖片說明： AlienVault USM一站式儀表板，清楚呈現所有資訊

BILLOWS TECHNOLOGY

CYBERSECURITY & COMPLIANCE

以情資戰勝勒索軟體

勒索軟體難以偵測，但並非無法戰勝，透過 AlienVault USM 的進階威脅偵測，將威脅止步於初期入侵階段。

主要功能與效益

資產盤點

透過主動和被動的網路盤查機制，產出環境內的資產清單、基礎結構和軟體清單。

行爲監控

監控本地、雲端環境、與應用程序中的使用者及特權活動，識別可疑行爲和潛在威脅。

安全性評估

主動式網路掃描以及不間斷的漏洞監控，找出您網路上較易於受攻擊的系統並進行事件關聯與管理。

SIEM

提供事件管理與關聯功能以及事件分析數據報告。配合威脅情資打擊 APT 攻擊等行爲。

入侵檢測

透過網路 IDS 以及主機 IDS 功能，偵測您的網路以及主機內部的惡意流量與行爲。

威脅情資資料庫

由 AT&T AlienLabs 維護的全球最大威脅情資交流平台，實現全球性的聯防體系。

安全和合規報告

包含標準內建與可自定義的報告，利於檢視是否符合資安框架與法規標準。

官網
http://billows.tech/home

LINE
@vri4754n

信箱
sales@billows.com.tw

電話 / 傳眞
02-25623952 / 02-25363763

地址
台北市中山區新生北路二段29之1號12樓