情資驅動資安維運平台

以情資與自動化爲主軸，協助企業進行全方位監控

新型態攻擊崛起 —— 資安思維再轉型

近年來各種資安事件不斷頻傳，網路安全開始受到各級機關、企業所關注，紛紛加碼資安預算，在網路環境中部署了各種不同功效的資安設備，以期阻止資安事件的發生。然而資安設備之間多是獨立運作，並依靠已知特徵去進行防護，對於零日攻擊或是APT等新型態攻擊幾乎是毫無招架之力，因此資安防護的思維轉型勢在必行。

情資賦能 —— 阻敵於外

面對日新月異的攻擊手法，唯有掌握更多更新的威脅情資才能有效防禦。All In One SOC針對防火牆、入侵防禦設備、或是交換器以及路由器等資安與網路設備日誌進行蒐集與保存，同時以豐富且即時更新的資安威脅情資，透過事件紀錄的分析找出潛在的威脅事件，在第一時間進行損害控管，找出威脅源頭進行防堵。

Billows All In One SOC 運行架構

資安防護七步驟

Billows All In One SOC

01

資料蒐集

部署Billows All In One SOC，記錄設備日誌並監控網路流量。

02

情資整合

匯集國內外資安威脅情資以及企業內部情資，形成資安戰情大數據。

03

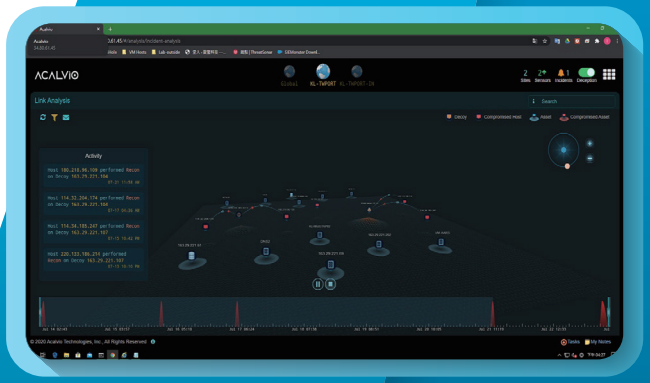
即時分析

針對資安事件進行威脅分析，提供風險等級、來源 IP、目的 IP、事件名稱等資訊。

0

行動

整合常見
時通報管
事件反應



入侵誘捕系統掌握攻擊者動態

透過情資牆即時阻擋黑名單來源

04

動告警

通訊APP，即
理人員，縮短
時間。

05

區域聯防

整合資安設備，自動變更資安設備防護政策，並且即時通知資安管理人員知悉。

06

事件回應

應變小組針對威脅分析結果進行緊急應變，第一時間降低損害。

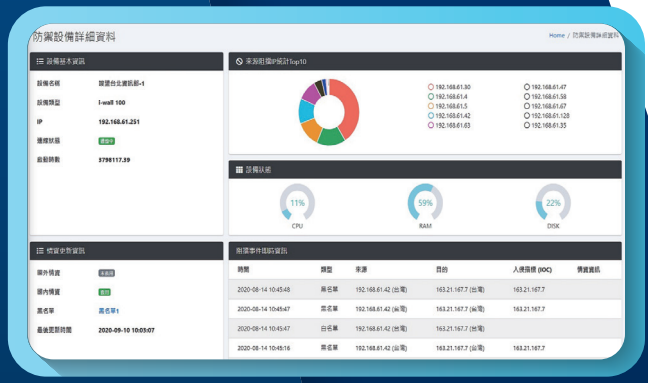
07

戰情中心

視覺化情資分析儀表板，讓資安管理者快速判讀與檢討資安策略。

BILLOWS TECHNOLOGY

自動化事件通報縮短反應時間



一站式儀表板即時呈現資安資訊

Billows 3A 防禦策略

Active · Analysis · Automation

外部入侵
智慧主動防禦服務

發展創新智慧化
主動式資安防禦模式

內部異常
智慧分析預警服務

首創全國行爲分析
資訊安全應用典範

資安事件
自動化通報服務

提供自動化
資安事件通報機制

All In One SOC 六大功能

監控資訊整合

以大數據資料收集功能爲基礎，能夠將進行資料分析、回應等不同任務之產品資訊整併，提供單一管理介面。

資安監控關聯規則

搭載AT&T提供的SIEM關聯告警規則，可自動更新與手動撰寫，協助管理者分辨可疑的APT攻擊提高監控時效性與有效性。

自動化事件通報

可進行自動化事件通報，協助從通報單產生至事件結案之流程管理，其資料格式均配合行政院資安會報訂定之規範。

威脅情資即時整合

以AT&T威脅情資爲主軸，整合國內外情資。協助釐清各項告警資訊，第一時間排除潛在威脅。

主動式防禦情資牆

以自動更新機制同步最新的惡意IP/URL資訊，針對網路流量進行即時比對，當發現惡意名單時可立即進行阻擋，減少釣魚網站之類的威脅事件發生。

端點威脅鑑識分析

端點威脅一向是同類型產品之缺口，本產品可針對端點威脅進行偵測分析，協助企業進行全方位監控。

關於竣盟科技

竣盟科技致力於協助客戶落實資安法規遵循，協助管理者在資訊整合等相關技術能夠無縫接軌原有業務，除了將法規制度與實際IT維運進行有效且合理的整合外，同時發展自動化流程，提升反應效率。透過自動化與資訊可視化，讓管理者能輕鬆處理法規相關的作業，改善資安狀況。

聯絡人　鄧小姐

聯絡電話　02-2562-3952

聯絡信箱　desiree@billows.com.tw

竣盟科技 網站

竣盟科技 Facebook 粉絲專頁

竣盟科技 Line@

BILLOWS

竣盟科技股份有限公司

CYBERSECURITY

COMPLIANCE

資安法遵

All In One SOC

Protect Your Business