Billows 資通威脅代管雲端MSSP服務

BILLOWS 竣盟科技股份有限公司

以協助企業符合資安法規為出發點的整合式資安事件監控服務

繼承了竣盟科技過往產品的特色，其核心監控機制是以威脅情資作為動力，搜集了國內外不同來源的資安情資，並進行匯聚與過濾，從而萃取出高價值的可用情資，情資來源包含了TWCERT以及全球電信聯盟等不同企業或組織，同時也可協助整合各大領域ISAC所提供的情資，運用在不同的監控環境。

資料接收器

- 利用代理程式方式進行資料收集，提供線上即時資安威脅偵測監控服務

應變回應

- 系統7*24監控
  導入Billows UCM 服務平台架構中相關威脅偵測及事件分析+E2產品，並由系統自動監控偵測與進行主動應變
- 專家5*8 情資判斷分析
  資安專家於線上5*8判斷事件威脅程度並提供相關威脅情資資訊，以協助資安人員精確處置
- IM發送即時通知
  整合社群軟體如Line APP，發送即時告警

異常告警種類

- 系統入侵(System Compromise)」
- 惡意程式植入(Exploitation & Installation)
- 網路攻擊(Delivery & Attack)
- 網路探測與偵查(Reconnaissance & Probing)
- 網路環境感知(Environmental Awareness)
- 使用者異常行為查測

分析能力與主動式異常行為警訊通知

- 系統提供的智能分析規則（Directive）功能，包含功能管理頁面與規則設定能力
- 即時監控網路流量，監控各類通訊協定和IP狀況的異常網路行為
- 提供主動式事件警示機制，可設定規則(Policy)以控制不同條件下的事件通知或處理方式，如：Email通知或開立事故單…等

	Essential (ET)	Enterprise (EP75)
資通安全威脅偵測	* Network Pacakge analysis - 200Mbps(網路封包分析) * SIEM(資訊安全事件分析與管理) * Billows Security Lab Threat Intelligence * Correlation 250 EPS * 主機行為監控 - 5A * 資安情資分享	* Network Pacakge analysis - 1000Mbps(網路封包分析) * SIEM(資訊安全事件分析與管理) * Billows Security Lab Threat Intelligence * Correlation 1000 EPS * 主機行為監控 - 75A * 資安情資分享
資通威脅代管雲端MSSP服務	* 事件追蹤分析與管理 * 資安告警警訊即時通知(Line模組/Email) * 5x8資安告警問題諮詢服務(Email/電話/Line模組) * 提供季報 - 4次/年(不提供on-site 報告)	* 事件追蹤分析與管理 * 資安告警警訊即時通知(Line模組/Email) * 5x8資安告警問題諮詢服務(Email/電話/Line模組) * 提供月報 - 12次/年(提供2次on-site 報告)

Billows Technology Co., Ltd. 竣盟科技股份有限公司
官網：http://billows.tech
電話：(02)2562-3952
地址：台北市中山區松江路129號6樓