如何建置SOC /ISAC資安通報系統

Gavin 鄭加海

Billows
一 竣 盟 科 技 一

- 台灣相關資安法規說明
- SOC＋ISAC通報規劃說明
  - 整合式資安分析(合規SOC)
  - 資安事件通報 (ISAC通報)

5/11通過資通安全管理法草案

首頁 > 政治 RSS

立院三讀資安法 未通報資安事件可罰500萬

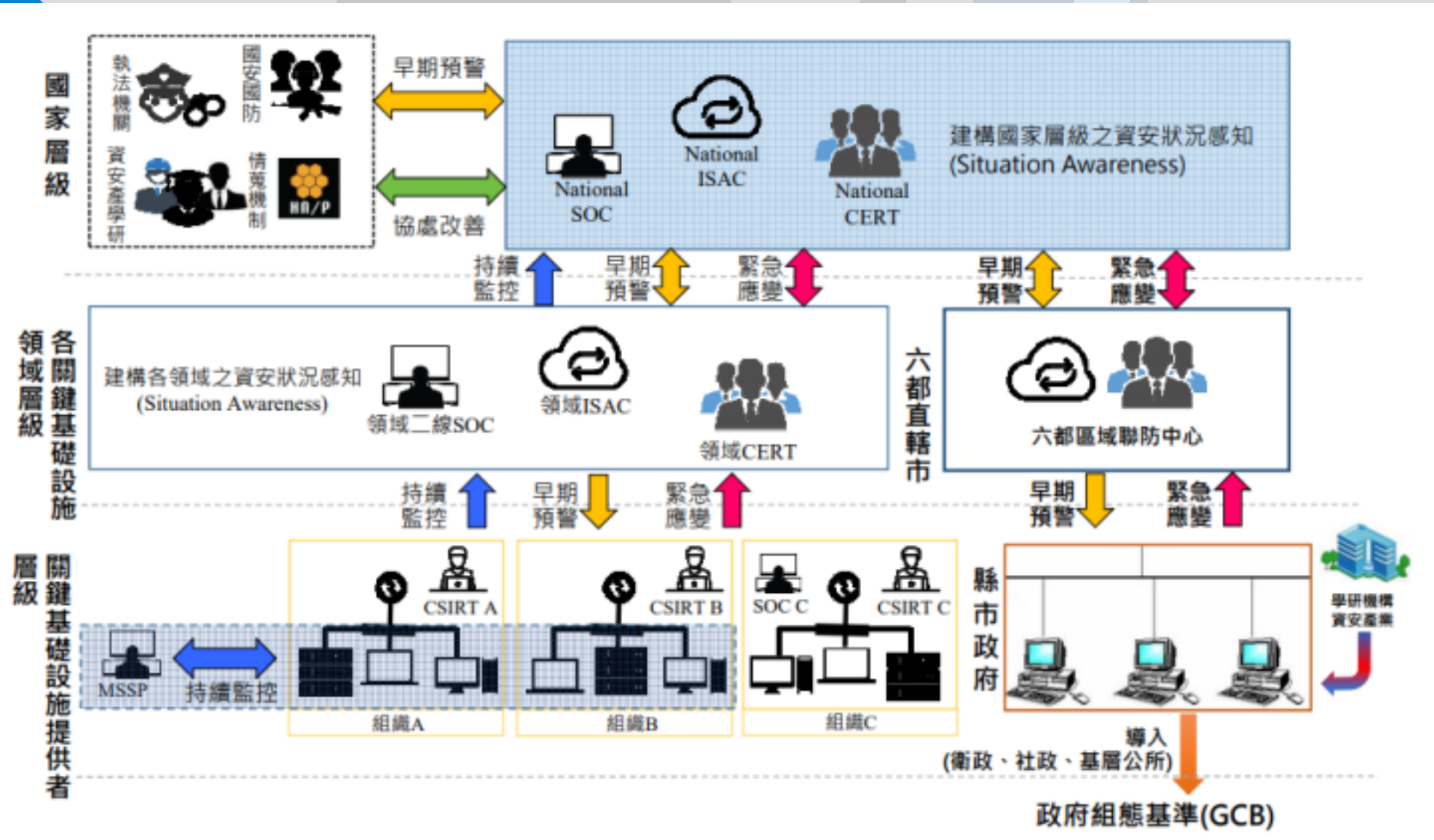
發稿時間：2018/05/11 13:58　最新更新：2018/05/11 14:56　字級：A- A+

Facebook　Google+　Twitter　Line

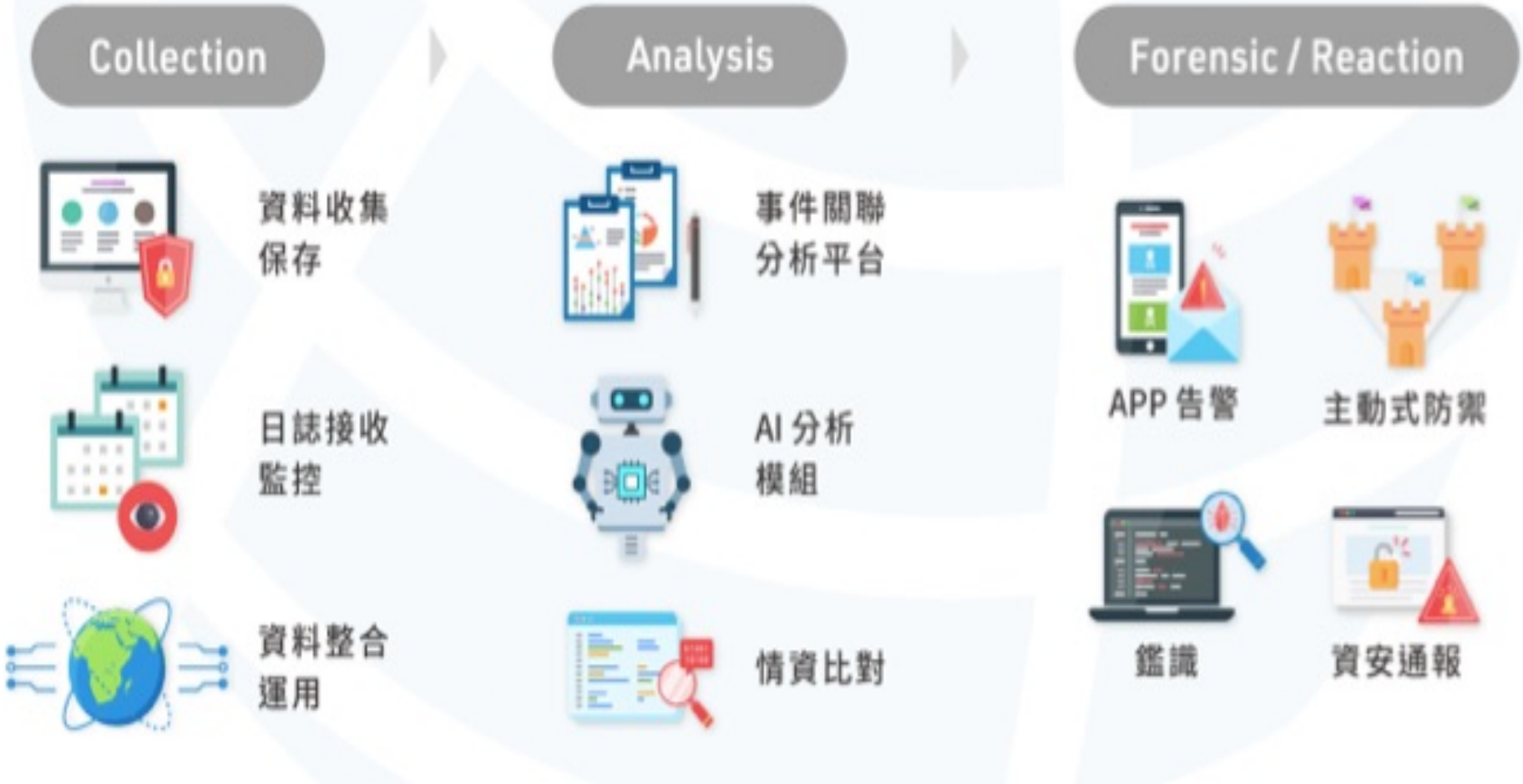
三讀條文明定，關鍵基礎設施提供者、公營事業、政府捐補助的財團法人等「特定非公務機關」，**應向主管機關提出資安維護計畫**，為因應資安事件，也**應訂定通報及應變機制**；知悉資通安全事件時，應向中央目的事業主管機關通報。

罰則部份，特定非公務機關未依規定通報資安事件，可處30萬元以上500萬元以下罰鍰，並得按次處罰；特定非公務機關未訂定、未實施資通安全維護計畫，或未依規定訂定資通安全事件通報及應變機制等，得令其限期改正，屆期未改正者，按次處10萬元以上100萬元以下罰鍰。

國家資安聯防體系架構


國家層級
執法機關
國安國防
資安產學研
情蒐機制
早期預警
協處改善
National SOC
National ISAC
National CERT
建構國家層級之資安狀況感知
(Situation Awareness)
持續監控
早期預警
緊急應變
早期預警
緊急應變
各關鍵基礎設施領域層級
建構各領域之資安狀況感知
(Situation Awareness)
領域二線SOC
領域ISAC
領域CERT
六都直轄市
六都區域聯防中心
持續監控
早期預警
緊急應變
早期預警
緊急應變
關鍵基礎設施提供者層級
MSSP
持續監控
CSIRT A
CSIRT B
SOC C
CSIRT C
組織A
組織B
組織C
縣市政府
學研機構
資安產業
導入
(衛政、社政、基層公所)
政府組態基準(GCB)

CI: SOC +ISAC 通報規劃



Billows
竣盟科技

整合式資安分析平台
(合規SOC)

Billows
一 竣 盟 科 技 一

國家資通安全技術與服務管理計畫 SOC 參考指引

功能架構	需求描述
資安警訊管理	能提供外部資安情資蒐集如CVE與惡意來源IP資訊比對 1. Open Threat Exchange
資安弱點管理	能依據弱點掃描或滲透測試的資料提供，確保系統沒有可遭利用的弱點，提升所監看的資安事件之有效性
資安設備管理	能定期偵測設備日誌接收狀態與效能 1. 資安設備定期更新 2. 資安設備日誌檢視 3. 設備異動管理
資安事件監看	能將大量的資安事件資料，篩選出極少數需要注意的，可能形成事故 的資訊，供監看人員進行分析 1. 系統訊息過濾與分析 2. Threat Intelligence
資安事故處理	1. 受害主機的鑑識與分析 2. 相關日誌與流量紀錄分析 3. 事件處理的相關記錄

About Alienvault

- Founded in 2007 and headquartered in San Mateo, CA with offices in Austin, TX; Madrid, Spain; Granada, Spain and Cork, Ireland
- Over 8,000 commercial customers
- More than 500 MSSP partners
- 350+ employees worldwide
- Backed by premier investors

Billows
一 竣 盟 科 技 一

We’re Trusted & Verified

- Aligned with NIST Cybersecurity Framework (NIST CSF)
- PCI DSS Level 1 Service Provider
- ISO 27001:2013 Certified Compliant*
- SOC 2 Type 2 Certified Compliant
- Attestation of HIPAA Compliance
- Certified Azure & AWS Advanced Technology Partner

HIPAA Compliant

PCI DSS Level 1 Service Provider

SOC 2 Type 2 Certified

Microsoft Azure Certified

amazon web services Partner Network
ADVANCED TECHNOLOGY PARTNER

Billows 一竣盟科技

Threat Intelligence

AlienVault Labs Threat Intelligence Update for USM Anywhere: April 8 - April 14, 2018

Announcement

AlienVault Labs Threat Intelligence Update for USM Anywhere: April 1 - April 7, 2018

Announcement

AlienVault Labs Threat Intelligence Update for USM Anywhere: March 25 - March 31, 2018

Announcement

AlienVault Labs Threat Intelligence Update for USM Anywhere: March 11 - March 17, 2018

Announcement

AlienVault Labs Threat Intelligence Update for

jkisielius
April 20

0

171

jkisielius
April 20

AlienVault Labs Threat Intelligence Update for USM Anywhere: April 29 - May 5, 2018

jkisielius
LITTLE GREEN ALIEN
May 11

5 10 25 +8

MESSAGE

in AlienVault USM Anywhere > AlienVault Threat Intelligence Updates

New Detection Technique – GPON Authentication Bypass (CVE-2018-10561)

This GPON vulnerability was publicly announced on May 3. It affects GPON routers and allows an attacker to bypass authentication and consequently perform Remote Code Execution via HTTP requests to the router. The HTTP requests only need to have '?images/' appended at the end of the URI to avoid authentication in the vulnerable system and take control of the router.

We've updated the 'Client Side Exploit – Known Vulnerability' correlation rule to detect this activity.

Related content in Open Threat Exchange: https://otx.alienvault.com/indicator/cve/CVE-2018-10561

New Detection Technique – DNN DNNPersonalization Cookie RCE Attempt (CVE-2017-9822)

This vulnerability affects DotNetNuke (DNN) software versions prior to 9.1.1. The exploit allows privilege escalation, granting Remote Code Execution through a particular setting of the DNNPersonalization value in the cookie. Despite the existence and awareness of the vulnerability, no exploits or Proof of Concept (POC) have been identified or made public.

We've updated the 'Client Side Exploit – Known Vulnerability' correlation rule to detect this activity.

Related content in Open Threat Exchange: https://otx.alienvault.com/indicator/cve/CVE-2017-9822

OTX (Open Threat eXchange)

To provide deeper and wider insight into attack trends and bad actors, the AlienVault Labs Security Research Team leverages the power of the Open Threat Exchange® (OTX™)—the world's first truly open threat intelligence community. This community of security researchers and IT professionals collaborate and share millions of threat artifacts as they emerge "in the wild," so you get global insight into attack trends and bad actors that could impact your operations.

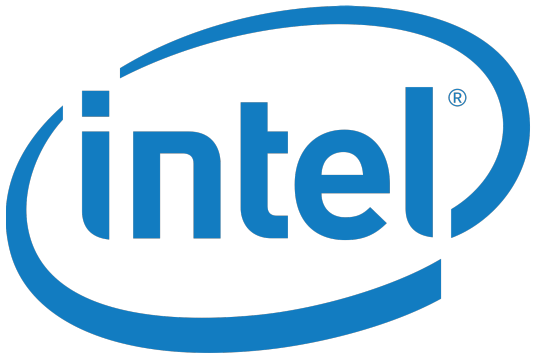
Learn More About Threat Intelligence ›

OVER 14 MILLION THREAT INDICATORS CONTRIBUTED **DAILY**

65,000+ PARTICIPANTS

140+ COUNTRIES

Open Threat eXchange 合作夥伴

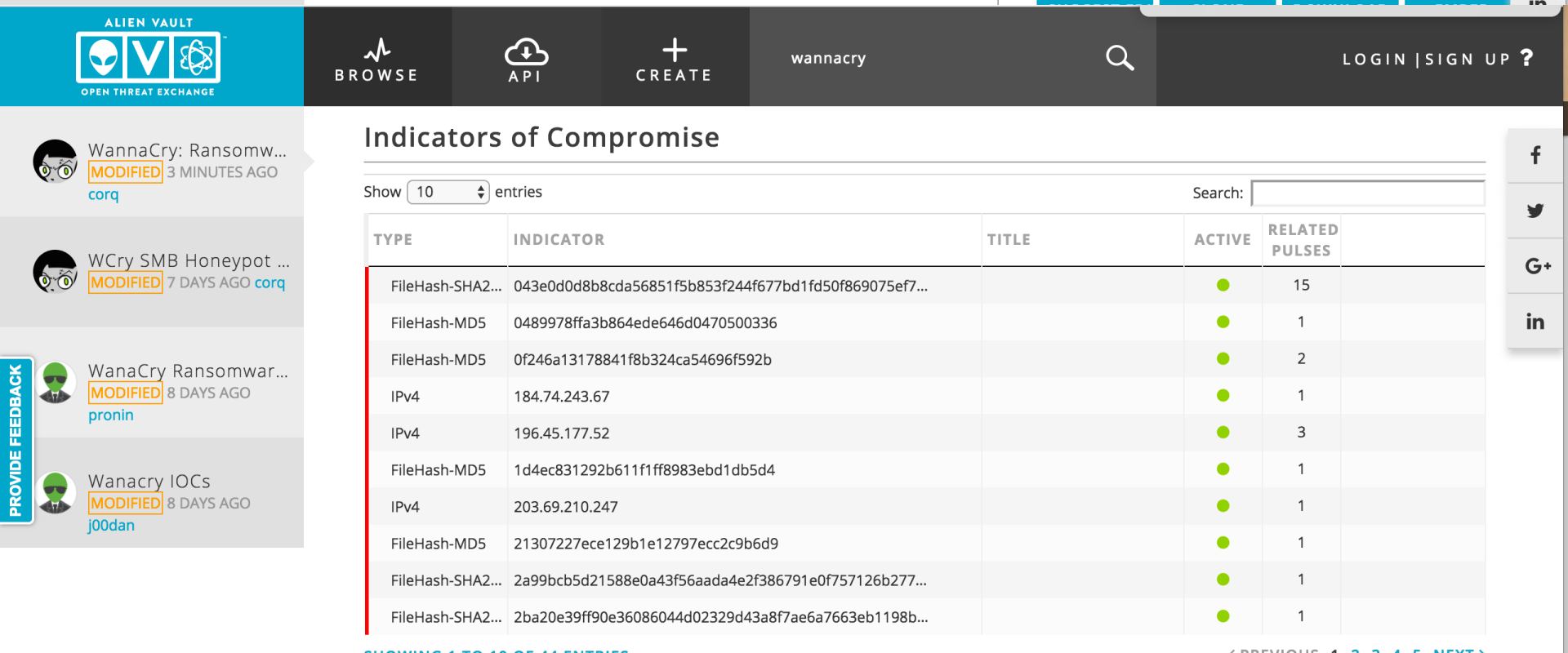


SANS:最受資安業界喜愛情資來源格式

- Open Threat Exchange (OTX)—51%
- Structured Threat Information Expression (STIX)—46%
- Collective Intelligence Framework (CIF)—39%
- Open Indicators of Compromise (OpenIOC) framework—33%
- Trusted Automated eXchange of Indicator Information (TAXII)—33%
- Traffic Light Protocol (TLP)—28%
- Cyber Observable eXpression (CybOX)—26%
- Incident Object Description and Exchange Format (IODEF)—23%
- Vocabulary for Event Recording and Incident Sharing (VERIS)—20%

OTX is very popular tool, with 51% of respondents using it. And CIF is also well-used, at 39%. While OpenIOC is in use by 33% of organizations, the clear majority uses the set of standards that include STIX, TAXII and CybOX. All of these standards and tools are still very much works in progress; however, the author has seen STIX and TAXII most commonly in enterprise organizations.

內網流量分析勒索軟體
WannaCry



AlienVault 內建軟體功能模組

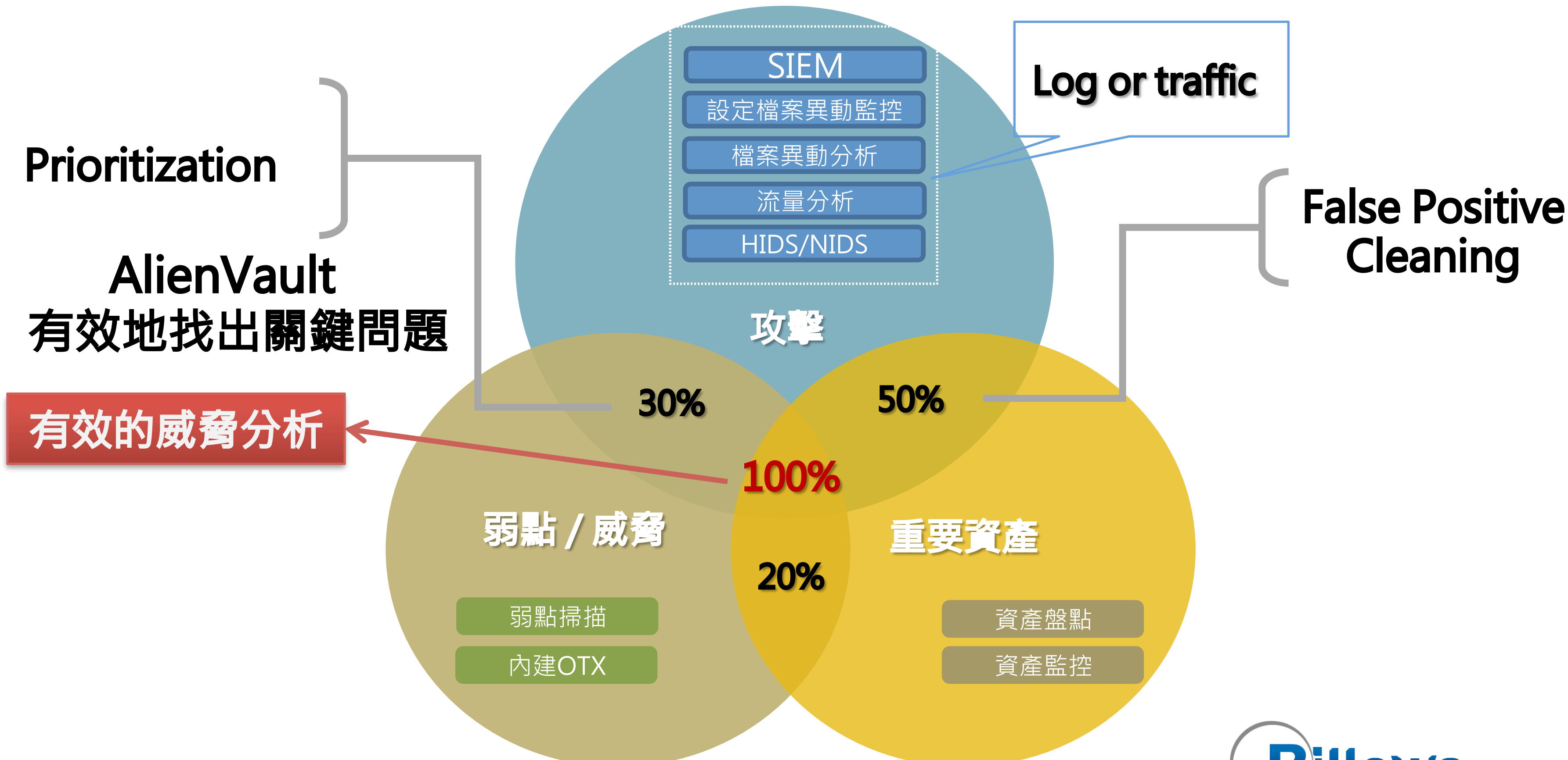
功能架構	需求描述
全球資安情資 OTX (資安警訊管理)	AlienVault Open Threat Exchange（OTX）是世界上最權威的開放式威脅信息共享和分析網絡。OTX提供對全球威脅研究人員和安全專業人員的社區的開放捷徑，在140個國家/地區有超過50,000名參與者，每天貢獻超過400萬個威脅指標。
資安事件管理 SIEM (資安設備管理) (資安事件監看)	A.統一和協調的安全監控 B.簡單使用的安全事件管理和報告 C.持續的威脅情報 D.快速部署 E.多個安全管理功能的單一個控制台
日誌保存Logger	A.數位簽名保存:確保可接受性作為法庭的證據 B. 日誌壓縮 降低存儲成本。 C.集中搜索輕鬆查找感興趣的數據。 D.中央保留策略實施公司或法規數據保留要求
權限管理	A.實體關聯 - 將用戶與結構樹中的實體相關聯 B.允許的資產 -實體關聯包括允許用戶查看的資產。此功能的作用類似於實體內的過濾器或關聯上下文 C.模板 - 授予對USM Appliance Web界面不同部分的訪問權限。模板是應用或選擇UI的哪些部分可供用戶訪問的直接方式。
弱點掃描 (資安弱點管理)	弱點掃描的功能，用於定義，識別，分類和優先處理系統中的漏洞。用於評估IT漏洞和確定響應緊急程度。弱點掃描系統CVSS, 此系統將嚴重性分數分配給弱點。範圍從0到10，其中10是最嚴重的。

AlienVault 內建軟體功能模組

功能架構	需求描述
內網行為分析 (資安事故處理)	A. 內網惡意行為\惡意中繼站連線分析 允許安全分析師對網絡流量執行完整的協議分析，從而可以完全重放潛在破壞期間發生的事件。 B.服務和基礎設施監控:提供對特定係統運行的服務的持續監控。定期或根據需要，探測設備以確認該服務仍在運行且可用。 C. NetFlow分析無需完整數據包捕獲所需的存儲容量即可執行網絡行為分析。 NetFlow分析提供與使用哪些協議，哪些主機使用協議以及帶寬使用相關的高級趨勢。
報表	USM Appliance報告包含兩個基本組件： A. 模塊定義對數據庫或檔案系統的查詢，以便檢索表和圖生成所需的數據。 B.佈局定義報告的圖形方面，例如徽標，頁眉和頁腳以及顏色方案。
Ticket System (資安事故處理)	事件管理包含有關檢測到的警報或您要在工作流中管理的任何其他問題的信息。在處理警報和事件時，最佳做法是始終通過USM設備資安事件流程管理系統或通過您自己公司的資安事件流程管理系統（如果適用）創建事件單來跟踪問題的進度和見解。創建警報或事件的票證不僅可以幫助您進行未來的調查，還可以創建審計跟踪來跟踪您所看到的內容，採取的操作以及跟踪問題的進度。
合規管理	經認證符合PCI DSS，HIPAA, ISO27002和SOC 2 等標準，可在合規認證過程中為您提供保證並減輕日誌存儲的負擔 ,在單個控制台中自動執行日誌收集，分析和事件關聯，提醒您異常或法規合規相關活動。 支援法規：DFARS, FREPA, FISMA, GLBA, HIPAA, ISO27002, NERC, PCI, SOX
事件回應	系統可以針對特定事件作下列自動回應 1. Email告警 2. 開事件單 3. 防火牆互動 4. 簡訊 (option) 5. 手機APP(option): Telegram, Slack, Line

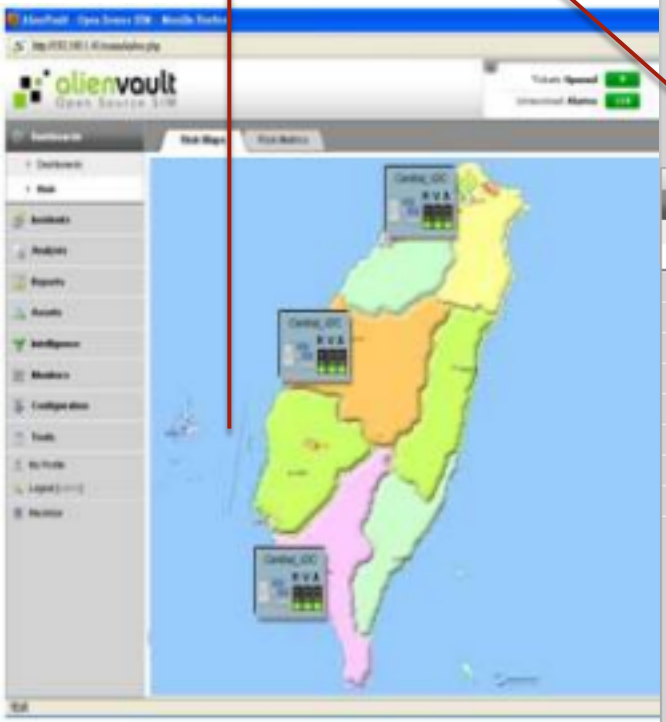
Threat Intelligence Correlation

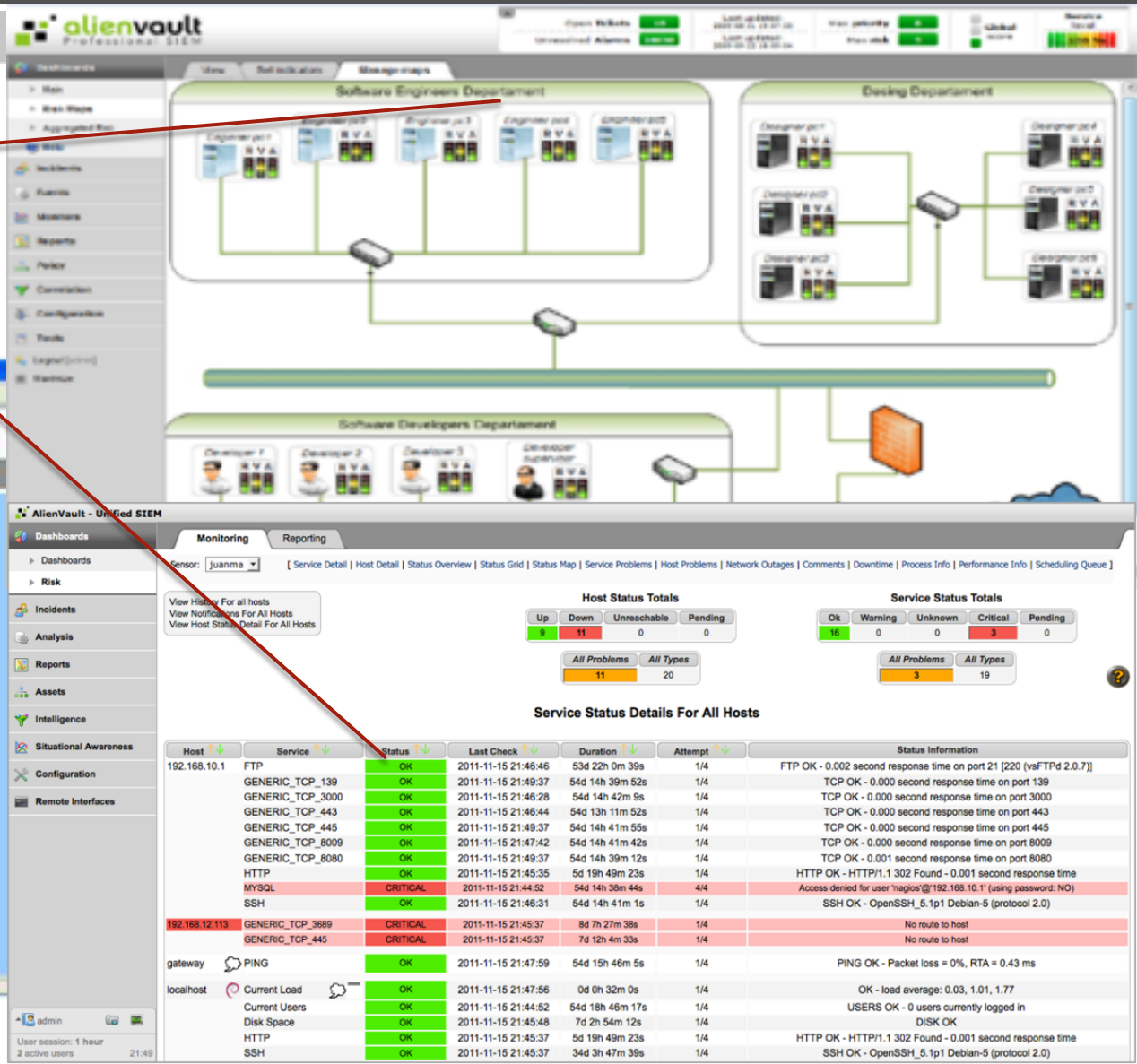
本題告警固然重要，自動發現真實告警威脅與基關鍵需求



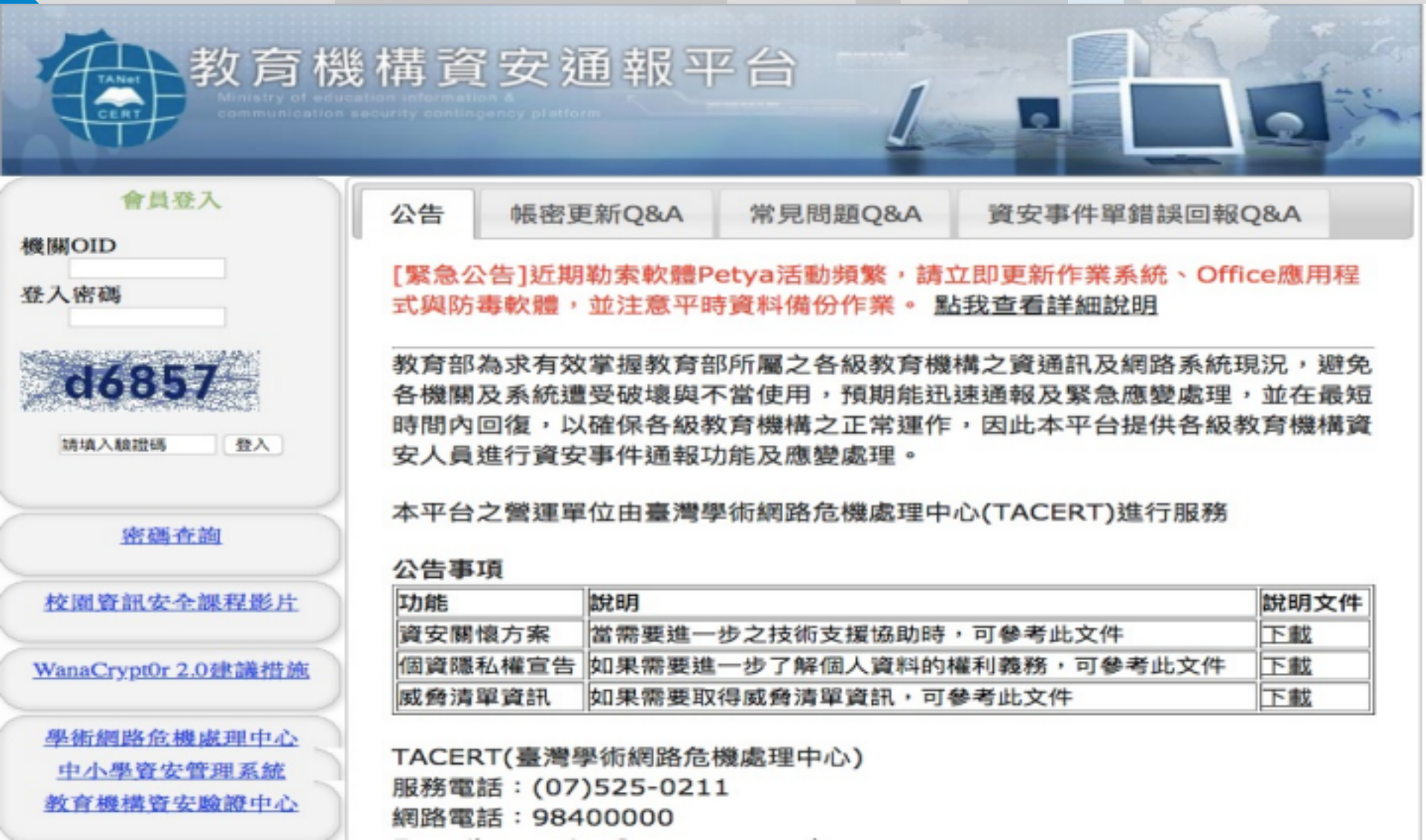
AlienVault 整合資料儀表板

清楚顯示資料中心的
狀況以及詳細資訊

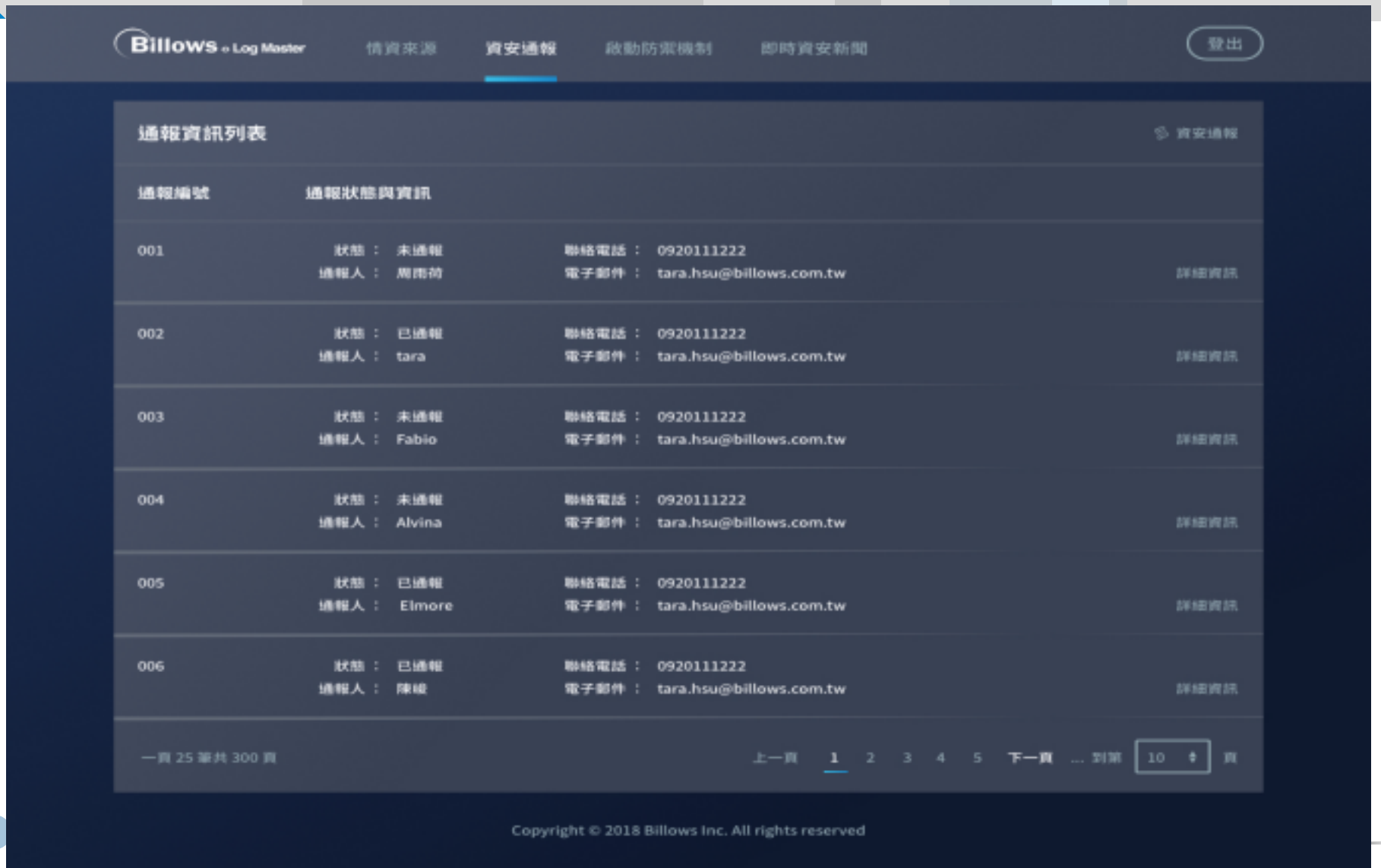




資安事件通報(手動)


教育機構資安通報平台
Ministry of education information & communication security contingency platform
會員登入
機關OID
登入密碼
d6857
請填入驗證碼
登入
密碼查詢
校園資訊安全課程影片
WanaCrypt0r 2.0建議措施
學術網路危機處理中心
中小學資安管理系統
教育機構資安驗證中心
公告
帳密更新Q&A
常見問題Q&A
資安事件單錯誤回報Q&A
[緊急公告]近期勒索軟體Petya活動頻繁，請立即更新作業系統、Office應用程式與防毒軟體，並注意平時資料備份作業。 點我查看詳細說明
教育部為求有效掌握教育部所屬之各級教育機構之資通訊及網路系統現況，避免各機關及系統遭受破壞與不當使用，預期能迅速通報及緊急應變處理，並在最短時間內回復，以確保各級教育機構之正常運作，因此本平台提供各級教育機構資安人員進行資安事件通報功能及應變處理。
本平台之營運單位由臺灣學術網路危機處理中心(TACERT)進行服務
公告事項
功能 說明 說明文件
資安關懷方案 當需要進一步之技術支援協助時，可參考此文件 下載
個資隱私權宣告 如果需要進一步了解個人資料的權利義務，可參考此文件 下載
威脅清單資訊 如果需要取得威脅清單資訊，可參考此文件 下載
TACERT(臺灣學術網路危機處理中心)
服務電話：(07)525-0211
網路電話：98400000

資安事件通報(自動)


Billows Log Master
情資來源
資安通報
啟動防禦機制
即時資安新聞
登出
通報資訊列表
資安通報
通報編號
通報狀態與資訊
001
狀態： 未通報
通報人： 周衍荷
聯絡電話： 0920111222
電子郵件： tara.hsu@billows.com.tw
詳細資訊
002
狀態： 已通報
通報人： tara
聯絡電話： 0920111222
電子郵件： tara.hsu@billows.com.tw
詳細資訊
003
狀態： 未通報
通報人： Fabio
聯絡電話： 0920111222
電子郵件： tara.hsu@billows.com.tw
詳細資訊
004
狀態： 未通報
通報人： Alvina
聯絡電話： 0920111222
電子郵件： tara.hsu@billows.com.tw
詳細資訊
005
狀態： 已通報
通報人： Elmore
聯絡電話： 0920111222
電子郵件： tara.hsu@billows.com.tw
詳細資訊
006
狀態： 已通報
通報人： 陳緯
聯絡電話： 0920111222
電子郵件： tara.hsu@billows.com.tw
詳細資訊
一頁 25 筆共 300 頁
上一頁 1 2 3 4 5 下一頁 ... 到第 10 頁
Copyright © 2018 Billows Inc. All rights reserved

Q & A

Billows
一 竣 盟 科 技 一