SHIELDXTREME
微智安聯

X-Threat

情資威脅服務

佈署全球欺敵網路偵測點，建置弱點場域誘使駭客發動攻擊，採主動式情資追擊，跨時區且零時差地與國際資安組織跨域合作進行情資交換，24 小時快速發佈預警式資安情資。

以雲端平台佈建 M.E.S.H. 系統，進行資料匯集與多維度的資安數據分析，並透過惡意程式沙箱分析及資料關聯性分析進行情資加值，萃取與確認以驗證情資有效性，協助進行資安風險管控。

- 佈建全球欺敵網路高達 20 個偵測點。
- 全域資安威脅偵測，掌握 10 億筆紀錄。
- 跨時區與零時差預警，24 小時快速發佈情資。
- 建構 M.E.S.H. 情資匯流，取得關鍵獵殺情資。
- 連結國際資安組織，提供 15 類主要威脅情資。
- X-Pot 行為分析閘道，全天候守護資訊安全。

Active Intelligence
國際情資平台、暗網、
營運資料與大數據分析、趨勢分析

Passive Intelligence
資安事件、新聞、社群網路、訊息分析

15 類主要威脅情資

情資類型	說明
Brute Force	暴力破解密碼異常行為資訊，多為真正攻擊的前兆。
Compromised	發佈已成為受駭者之資訊。
Scan	網路掃瞄等異常行為資訊，提供攻擊來源資訊。
Spam	提供垃圾郵件相關情資。
C2	提供殭屍網路惡意中繼站資訊。
Botnet	提供殭屍網路活動資訊。
Phishing	提供釣魚網路等相關資訊。
Suspicious	提供可疑的攻擊來源資訊。
DDoS	提供分散式阻斷服務攻擊來源資訊。
APT	提供 APT 攻擊相關資訊。
Crypto	提供資料外洩、加密貨幣挖礦活動等相關資訊。
Exploit	提供在攻擊行動中被使用的漏洞套件相關資訊。
Malware	提供惡意程式相關資訊。
Tor	提供匿名服務與洋蔥網路相關資訊。
Others (CI, Hacking Intelligence)	依特殊需求進行情資提供。 (如：關鍵基礎設施、產業別等特定類型)

情資服務方式

Files (via HTTPS)
透過檔案進行情資交換，情資檔案名稱固定格式並定期更新。
檔案格式：JSON

Restful API
平台或應用程式透過 API 進行資料交換，可定期進行自動化查詢，或依需求類型進行查詢。

TAXII
透過架設 TAXII Client 與 ShieldX TAXII Server 進行情資交換。
符合：STIX 2.0 (Global)、
N-ISAC (Taiwan)

Contact Us
service@shieldx.io

Official Website
https://www.shieldx.io/