資安通報平台威脅情報說明

當收到資安情資後，經適當且有效的系統調查後，並未發現有直接或間接證據可證明系統遭受到資安事件之威脅即可選擇 TII(**威脅情報**)。建議您在進行系統調查時進行下列步驟：

- 檢查系統或網路相關 LOG 資訊，查看是否有異常之處。
- 利用如 TCPVIEW 工具軟體或 netstat 指令來查看系統是否有開啟可疑之服務或是否有可疑之來源連線。
- 查看防火牆之連線記錄，確認是否有可疑之連線。
- 如果有設置入侵偵測軟體（IDS），進行查看是否有惡意的連線行為。