# SafeCove iSDA 強化 DNS 攻擊行為偵測平台(每年訂閱)

## 產品簡介

iSDA（Intelligent Security Detection Appliance）為本公司研發團隊針對 DNS 原始事件資訊所自主研發之系統，**該系統包含自行開發之人工智慧演算法，透過多種演算法模組之運算，偵測 DNS 異常行為，本平台將與網域名稱安全過濾服務形成雙重防護架構**，強化 DNS 攻擊行為偵測：

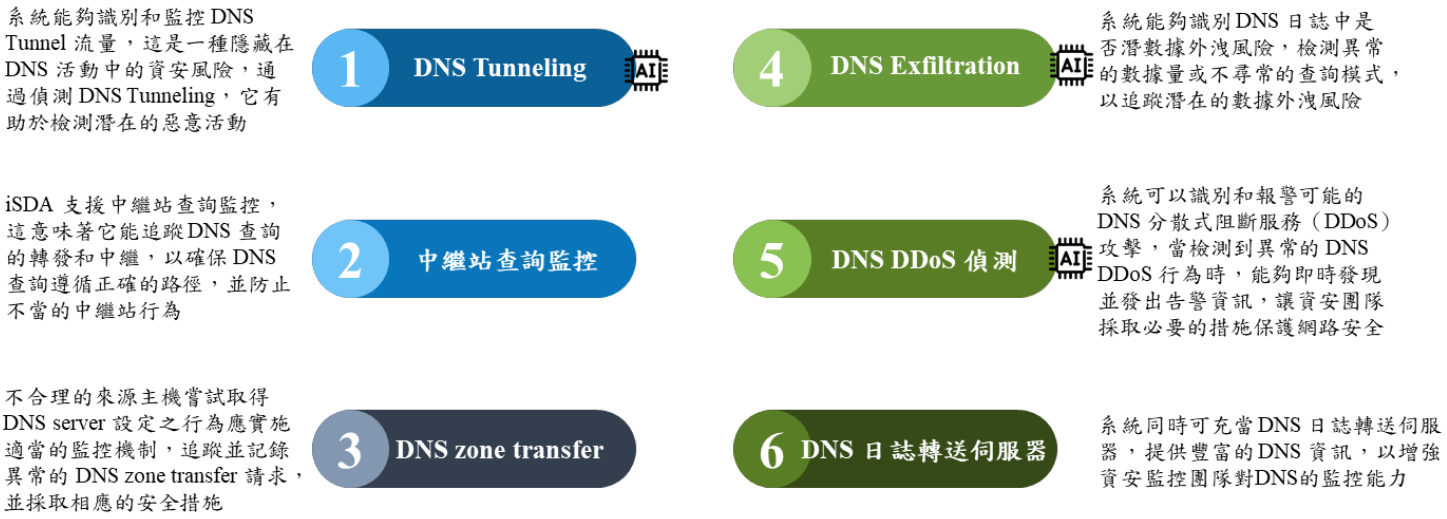


*圖1　iSDA 六大關鍵功能*

1. DNS Tunnel 異常行為偵測：
   系統能夠識別和監控 DNS Tunnel 流量，這是一種隱藏在 DNS 活動中的資安風險，通過偵測 DNS Tunneling，它有助於檢測潛在的惡意活動。
2. 中繼站相關查詢：
   iSDA 支援中繼站查詢監控，這意味著它能追蹤 DNS 查詢的轉發和中繼，以確保 DNS 查詢遵循正確的路徑，並防止不當的中繼站行為。
3. DNS zone transfer 之查詢行為：
   AXFR/IXFR 為 DNS zone transfer 使用的特殊查詢類型，若其它主機嘗試進行此類查詢，可能為駭客透過潛伏的受害主機進行資訊蒐集，此偵測會經過 profiling 動作，確認客戶環境中允許進行此動作的來源 IP。
4. DNS Exfiltration：
   系統能夠識別 DNS 日誌中是否潛數據外洩風險，檢測異常的數據量或不尋常的查詢模式，以追蹤潛在的數據外洩風險。
5. DNS DDoS 偵測：
   系統可以識別和報警可能的 DNS 分散式阻斷服務（DDoS）攻擊，當檢

測到異常的 DNS DDoS 行為時，能夠即時發現並發出告警資訊，讓資安團隊採取必要的措施保護網路安全。

6. DNS 日誌轉送伺服器

系統同時可充當 DNS 日誌轉送伺服器，提供豐富的 DNS 資訊，以增強資安監控團隊對 DNS 的監控能力。

本平台將以貴單位 DNS 網路流量作為主要偵測標的，並將於資安監控區內，建置一台專用的伺服器，以此進行 DNS 偵測作業。本作業需請貴單位配合在 Switch 上設定，將網路流量導向至資料收集設備，收集方式可採 SPAN（Port Mirroring），或使用 TAP 設備取得鏡像資料，以利 AI 模型進行資料特徵萃取。iSDA 偵測 DNS 行為之流程如下圖所示。

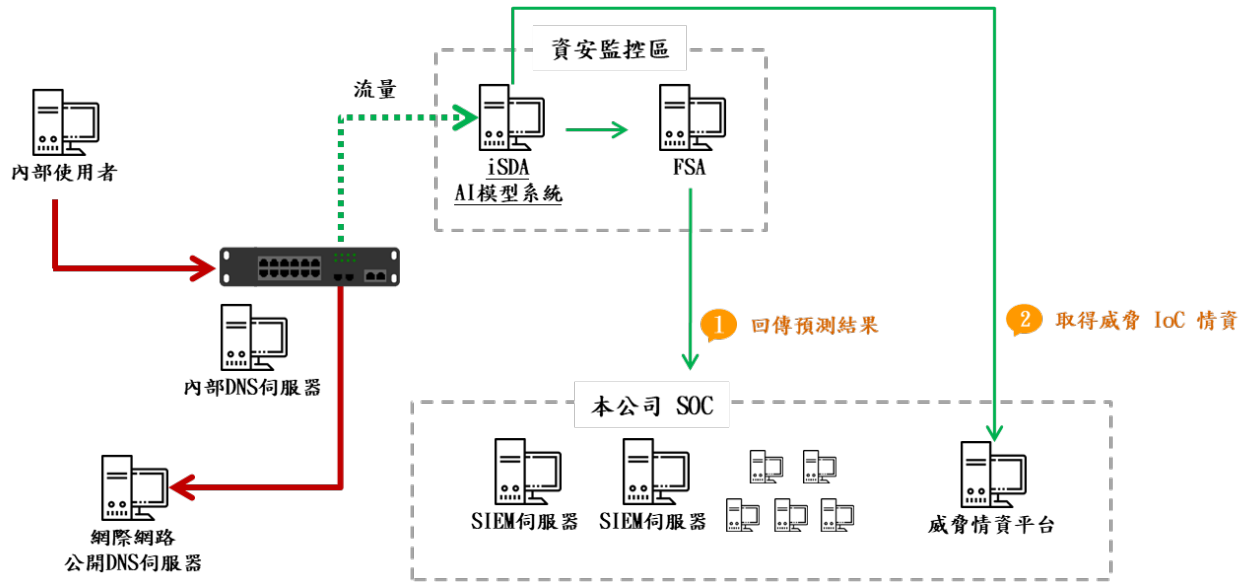


*圖2　iSDA 偵測 DNS 流程示意圖*

如上圖所示，本平台將 iSDA 產出的偵測結果，回傳至本公司 SOC 監控中心，提供數據予 SOC 監控人員進行規則關聯之設計與判斷依據，將可有效偵測惡意連線或行為，強化 DNS 攻擊行為之偵測。

# 產品功能說明

| 項目 | 內容說明 |
|---|---|
| 產品功能 | |
| iSDA 強化 DNS 攻擊行為偵測平台 | ● DNS Tunnel 異常行為偵測<br>● 中繼站相關查詢<br>● DNS zone transfer 之查詢行為 |

| 項目 | 內容說明 |
| --- | --- |
| | ● DNS Exfiltration<br>● DNS DDoS 偵測<br>● DNS 日誌轉送伺服器 |
| 技術支援 | |

## 產品授權

| 產品名稱 | 授權數量 |
| --- | --- |
| SafeCove iSDA 強化 DNS 攻擊行為偵測平台(每年訂閱) | 提供 iSDA 強化 DNS 攻擊行為偵測平台一年使用授權 |

## 產品售價

- NT$80 萬(含稅)

## 交付項目

- SafeCove iSDA 強化 DNS 攻擊行為偵測平台(每年訂閱)

## 平台硬體需求

| 項目 | 最低建議(<100Mb/s) | 建議（100Mb~1Gb/s） | 超高流量(>1Gb/s) |
| --- | --- | --- | --- |
| CPU | 8 core *2 | 12 core *2 | 16 core *2 |
| Memory | 32 GB | 64 GB | 128 GB |
| Storage | 2 TB SATA(SAS) (1 TB * 3, RAID5)<br>1.8 TB SATA(SAS) (600GB * 4, RAID5) | 6 TB SAS (2 TB * 4, RAID5) | 10 TB SAS (2 TB * 6, RAID5) |
| Ethernet | 1 Gigabytes Port *4 | 1 Gigabytes Port *4 | 1 Gigabytes Port *2<br>10 Gigabytes Port *4 |

# 預期效益

- 透過多種演算法模組之運算，偵測 DNS 異常行為，本平台將與網域名稱安全過濾服務形成雙重防護架構，強化 DNS 攻擊行為偵測