TSM NETDOM (Network Threat Defense & Orchestration Matrix)

網站資安聯防系統產品型錄

目錄

---

1. 前言：迎接新型態資安威脅挑戰

在數位化浪潮下，企業網站已成為營運的核心樞紐，同時也成為駭客攻擊的首要目標。傳統的資安防護措施，如防火牆（WAF）或入侵偵測系統（IDS），多屬被動防禦，依賴已知的攻擊特徵庫（Signature-based）。然而，面對今日運用人工智慧、變化多端且持續發動的自動化攻擊，此類防禦機制往往顯得力不從心。攻擊者利用殭屍網路（Botnet）中的 C&C（C2 命令與控制）伺服器，指揮大量受感染的設備發動滲透掃描、SQL 注入、暴力破解等攻擊，其 IP 位址頻繁更換，使得傳統的黑名單難以即時應對。

TSM NETDOM 網站資安聯防系統的誕生，正是為了顛覆此一困境。我們以「主動、智慧、聯防」為核心理念，打造出一套能夠自主學習、即時分享並協同抵禦的下一代網站資安解決方案，並提供彈性的部署方式，以滿足不同企業的資安政策與基礎設施需求。

2. 產品概述：什麼是 TSM NETDOM？

TSM NETDOM（NEtwork Threat Defense & Orchestration Matrix）是一款創新的資安聯防系統。它不僅是一個軟體或設備，更是一個可跨地域協作的威脅情資共享與協同防禦網路。系統透過輕量級代理程式（Agent）部署於您的網站伺服器上，持續監控所有進出的網路流量。

其核心使命在於：**利用深度學習技術，自動化辨識出正在對保護網域進行惡意探測或攻擊的駭客 C&C IP 位址，並在最短時間內將此威脅情資同步至所有聯防網路中的主機，實現「一處偵測，全域阻擋」的即時防護效果。**

3. 部署架構選項：雲端服務與地端本地部署

為適應企業多元化的 IT 環境與資安政策，TSM NETDOM 提供兩種主要部署模式：

A. 雲端服務版 (SaaS)

- **簡介：** 以訂閱制軟體即服務（SaaS）形式提供，由我方全權管理與維護

後端威脅情資平台。

- **架構：**
    1. **本地代理程式（Agent）：** 輕量級軟體，部署於每台需受保護的網站伺服器。
    2. **TSM NETDOM 雲端威脅情資中心：** 系統的核心大腦，位於高可用性、高防護等級的雲端資料中心。
- **運作方式：** Agent 將匿名的行為元數據（Metadata）加密傳送至雲端中心進行深度學習分析。一旦發現威脅，雲端中心會將阻擋指令秒級同步回所有相關的 Agent。
- **優勢：**
    - **快速部署：** 無需投資硬體或建設後端平台，安裝 Agent 即可上線。
    - **免維護：** 系統更新、效能擴充、資安防護均由我方負責。
    - **全球聯防：** 可輕鬆與其他雲端版客戶共享匿名化威脅情資，形成更廣泛的防護網絡。
- **適合對象：** 追求效率、希望降低維護負擔、IT 資源有限或主要應用已部署於公有雲/混合雲的企業。

B. 地端本地部署版 (On-Premises)

- **簡介：** 將完整的 TSM NETDOM 系統（包含威脅情資分析平台）部署於企業自有的資料中心內。
- **架構：**
    1. **本地代理程式（Agent）：** 與雲端版相同，部署於受保護的網站伺服器。
    2. **本地威脅情資管理平台：** 一套包含深度學習引擎、資料庫及管理介面的虛擬應用設備（Virtual Appliance），完全運行於您的內部網路。

- **運作方式：** 所有流量分析、威脅判斷、情資同步等過程，完全在您的內部網路中完成，資料無需離開企業環境。
- **優勢：**
    - **資料自主性：** 所有日誌、行為數據等敏感資訊均留存於內部，符合嚴格的資料落地（Data Residency）法規或內部資安政策。
    - **網路隔離：** 適合無法直接對外連線的關鍵基礎設施或高度機密環境。
    - **自訂聯防群組：** 可與關係企業（如集團子公司、緊密合作夥伴）建立專屬的私有聯防網路。
- **適合對象：** 政府單位、八大 CI 關鍵基礎設施機構或提供網路服務的產業或對資料主權和隱私有極高要求的的大型企業。

4. 核心功能詳解

4.1 AI 驅動之 C&C 伺服器 IP 自動辨識與阻擋

這是 TSM NETDOM 的最關鍵創新。系統的深度學習模型並非僅是分析單一封包內容，而是專注於辨識「攻擊行為特徵」。

- **行為特徵分析：** 模型會分析連線的頻率、模式、封包內容等多個個維度。
- **網路探測關聯：** 系統會關聯同一 IP 是否在進行網站接口掃描(Scanning)、服務旗標擷取（Banner Grabbing）等常見的攻擊前探測行為。
- **自動判斷與分類：** 經過模型計算，當惡意意圖的置信度超過預設閾值時，系統會自動將該 IP 標記為高風險 C&C 嫌疑位址。
- **即時阻擋：** 一旦判定為惡意 IP，Agent 會立即透過本機防火牆規則或與現有 WAF 整合，將該 IP 的所有連線阻斷。

4.2 全球/全域聯防，秒級同步威脅情資

TSM NETDOM 的強大之處在於其「聯防」機制。

- **雲端版：** 威脅情資可透過我方雲端中心，與其他（經授權的）客戶進行

匿名化共享，實現跨企業的全球聯防。

- **地端版：** 聯防範圍限於已部署本地平台並建立信任關係的內部網路或集團網絡 (如台北、東京、舊金山機房)。情資同步在內網完成，速度極快。
- 實現「一處偵測，全域阻擋」，讓攻擊者的 C&C IP 資源迅速失效。

4.3 彈性化管理：手動黑白名單與例外處理

- **手動新增黑名單/白名單：** 透過統一的命令列管理進行操作，不透過 HTTP 介面，不會有類似 WAF 設備的網頁管理系統被駭客攻陷 WAF 管理網站的問題。
- **紀錄與稽核：** 所有自動阻擋與手動調整的記錄皆完整留存。

4.4 主動防禦：使弱點掃描工具失效

- 能在掃描工具完成整個探測週期前，識別出其非正常的、系統性的請求模式，並立即阻擋掃描來源 IP。
- 結果是：**掃描工具將無法獲取完整的掃描報告**，大幅提高攻擊者難度。

5. TSM NETDOM vs. 傳統 IP 信譽評等服務

特性	TSM NETDOM	傳統 IP 信譽評等服務
情資來源	**第一手、內生性情報。** 直接來自對您企業網站的實際攻擊流量，百分之百相關。	**第二手、外部性情報。** 收集自公開威脅情資源或合作夥伴，可能包含大量與您無關的惡意 IP。
針對性	**極高。** 專注於「實際意圖攻擊您網站的 IP」。	**通用性。** 提供的是全球性的惡意 IP 清單，針對性較低。
時效性	**即時 (Real-time)。** 攻擊發生當下即可辨識並分享。	**延遲 (Hours or Days)。** 情資的收集、彙整、發布需要時間。
部署彈性	**高。** 提供雲端與地端兩種模式，適應不同需求。	**通常為單一形式 (雲端 API 或特徵碼更新)。**

6. 技術架構與運作原理

TSM NETDOM 採用統一的 Agent 與分層式後端架構：

1. **統一本地代理程式（Unified Agent）：** 無論雲端版或地端版，均使用相同的輕量級 Agent 軟體安裝於支援的作業系統中，簡化部署與管理。
2. **後端分析平台（Backend Platform）：**
    - **雲端版：** TSM NETDOM 雲端威脅情資中心。
    - **地端版：** 本地部署的威脅情資管理平台（虛擬應用設備）。

7. 雲端版與地端版系統需求

- **共通需求（Agent 端）：**
    - **伺服器 OS：** AlmaLinux 9/10+, Ubuntu 22.04+, Windows Server 2016+, 皆 x64 版本。
    - **資源需求：** CPU 核心數 ≥ 2，記憶體 ≥ 16 GB（視流量而定），硬碟空間 ≥ 20 GB。
- **雲端版特定需求：**
    - **網路：** Agent 需能透過 HTTPS/SSL 對外連線至 TSM NETDOM 雲端服務特定埠口。
- **地端版特定需求（平台端）：**
    - **硬體/虛擬環境：** 需預留足夠資源運行虛擬應用設備（建議配置：vCPU ≥ 8，記憶體 ≥ 32GB，儲存空間 ≥ 2TB，視受保護主機規模與日誌保留政策而定）。
    - **網路：** 內部網路需能讓 Agent 與管理平台通訊。
    - **需搭配 TSM WAF 及 WEB X-RAY 系統。**

8. 效益分析：為企業帶來的價值

- **降低資安風險與提升營運韌性。**
- **節省資安人力。**

- **符合合規要求：** 地端版特別適合有嚴格資料落地要求的法規。
- **部署彈性：** 可根據企業現狀選擇最合適的方案，無縫整合現有環境。

9. 成功案例

大型電信公司（採用地端版）

- **挑戰：** 因應規範，所有客戶資料與資安日誌不得落地境外，且需建立集團內部的聯防體系。
- **導入 TSM NETDOM 地端版後：**
    - 將平台部署於集團核心機房，旗下多家子公司的網站伺服器均安裝 Agent。
    - 成功在合規前提下，建立起集團內的私有聯防網絡。當官網遭受攻擊時，其他網頁服務網站立即獲得防護。
    - 滿足了內外部稽核對日誌留存與資安控管的要求。
    - 安裝部署數量超過 200 台，一年 365 天運作 0 失誤。

10. 服務與支援

我們提供全面的技術支持，並依據版本有所不同：

- **雲端版：** 7x24 平台監控、主動式威脅通報、自動化更新與維護。
- **地端版：** 遠端技術支援、平台版本更新服務、專業技術諮詢。

11.結論：打造堅不可摧的網站防護網

TSM NETDOM 提供兼具智慧與彈性的資安聯防方案。無論您傾向於擁抱雲端效率，還是堅持地端掌控，我們都能提供相對應的強大防護。立即聯絡我們的資安顧問，讓我們為您量身打造最合適的網站防護策略。

TSM Software Technology, Inc.
小松鼠軟體有限公司
新北市中和區景平路 288 號 13 樓之 15
Tel: +886-2-2941-5500
http://www.tsmst.com

TSM Software 小松鼠軟體