
WWW.NEITHNET.COM
SEEKER
MANAGED DETECTION AND RESPONSE
NEITHNET
Accelerate Your Insight

SEEKER

點亮威脅暗處
全面性的端點禦敵方案

如大海般廣闊且神秘的網路世界，我們時而悠遊於淺層海域，時而朝向深邃神秘處探索。然而，無論淺灘或深海，都藏匿著我們意想不到的風險與危機。現今的網路威脅，神秘、隱匿又詭譎，攻擊型態從以往的沿岸波濤演進到深海的暗潮洶湧，暗藏於企業內部，潛伏期極長，虎視眈眈準備竊取資料並加密勒索。然而在傳統IT資安架構之下，不易檢測這樣的威脅，並使IT人員疲於奔命調查重複事件，耗費大量成本與時間，最遺憾的是常常無法成功攔截。

NEITHSeeker託管式偵測與回應系統（Managed Detection and Response, MDR）協助企業以普遍可負擔的成本，透過隨時監控網路及端點資料，每天執行搜集資料，並加以分析、判斷與追蹤，釐清各式惡意跡象，即使是微小的警示，都有助及早發現並排除問題，持續不間斷守護企業珍貴的數位資產，讓客戶如同擁有一個專業資安團隊的防護效益，卻無須負擔維持一個專業資安團隊的高昂成本。

即時高品質情資

NEITHNET蒐羅網域中多種樣態的攻擊流量，並透過世界級IOC資料庫交換與各資料中心採集樣本及監控世界各地網路攻擊等，集結出深度暨廣度最豐富的網路流量資料，並由資深資安研究人員萃取出最即時、活躍的精準情資，正確判斷已知與潛藏的網路威脅。

威脅分析自動化

NEITHNET資安戰略實驗室 (NEITHCyber Security Lab) 運用人工智能技術，將目前及過去搜集的多維度情資，交叉關聯多重來源，分析及建構攻擊指標模型，勾勒完整的攻擊流程樣態，發展出威脅檢視指標，自動辨識網路惡意足跡，防止組織內的資安漏洞。

主動隔離檔案與端點

為有效防禦與控制日益劇增的勒索病毒攻擊，除了監控端點異常提權行為也時刻關注橫向移動，當偵測到特定可疑行為時，可將檔案隔離，抑或將端點逕行斷網阻止危害擴大。

APT 資安專家健檢

以精簡成本，即可享受資安鑑識專家服務，定期提供客戶網路健檢的報告，有助及早發現並排除風險。並依客戶狀況或需求，提供資安環境建構與補強策略分析、惡意軟體樣本分析等報告，以釐清惡意跡象。

高度整合各式平台，部署容易

高度支援多種平台(Windows、Linux、macOS)，安裝即可用無須多餘設定。

彈性搭載 NEITHDNS，安心暢遊網際

NEITHSeeker可與NEITHDNS進行端點與網域名稱系統伺服器聯防，將端點DNS Server指向NEITHDNS，當端點發出釣魚網站或惡意網站的解析請求，即可將惡意連線阻殺，並將瀏覽器頁面安全地導轉至告警頁面，防止惡意攻擊管道的建立與機敏資料的外洩風險。

點防護妥善率暨IT資產清查

騰曜網路科技的MDR搭載了輕量化的網路探針，被動式的搜集網路資料，在不影響網路品質的情況下，幫您捍衛網路疆界的安全。除了能偵測Agent的部署率，也能一併清查網路設備，在Layer 2、Layer 3規則不夠嚴謹的場域，容易滿佈私有設備與被遺漏的機器。當威脅來臨時，資安黑數將成為駭客躲藏的溫床，如時下最盛行的勒索軟體常在內網中橫向移動到處亂竄，造成寶貴資產落入駭客囊中，騰曜深知輕忽資安基礎的危害，有效幫助客戶減低曝險面積。

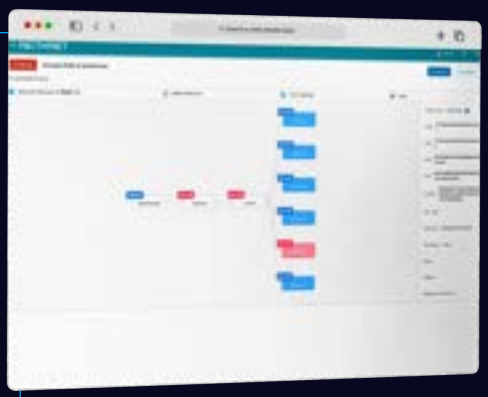
服務項目

7x24 全程監控

- 嚴重威脅事件即時通報
- 每週事件通報
- 每月完整報告
- 不限次數資安事件詢問
- 建立符合企業專有MDR規則

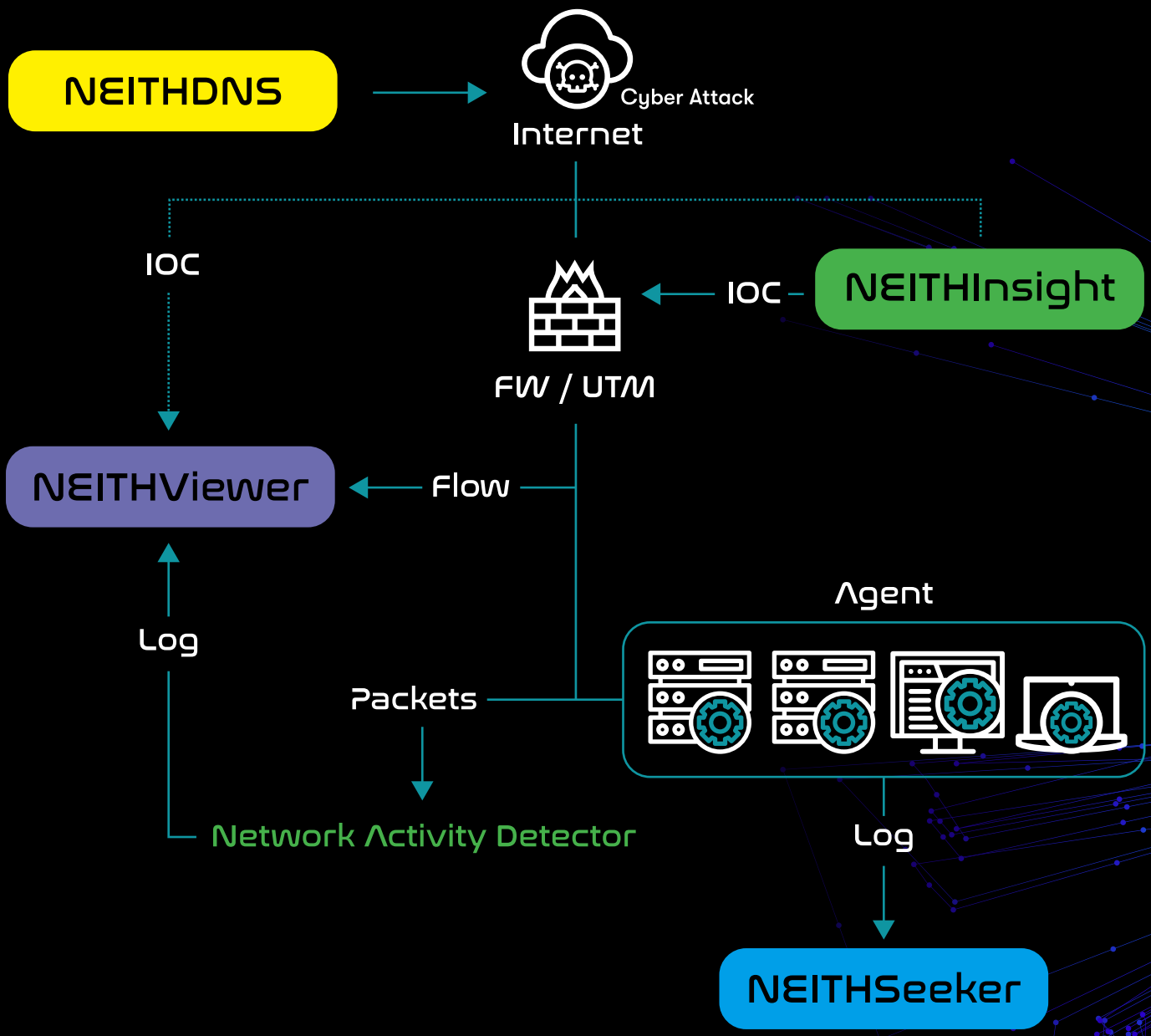
主要功能

- 端點系統分析
- 網路異常行為偵測（橫向移動）
- 儀表板可視化管理
- 主動隔離檔案與端點
- 自動化告警與通知
- 告警系統化(MITRE ATT & CK)
- 惡意釣魚網站偵測
- 程式行為可視化分析
- 世界級IOC資料庫
- 專家諮詢及事件分析報告



透過Process Tree分析快速找出可疑程序執行的過程，與使用的可疑指令內容。

NEITHNET Solution



About NEITHNET

騰曜網路科技(NEITHNET)專精於超前洞察隱匿的網路威脅，由一群熟稔網路攻防語言的熱血資安專家所組成，並設有世界級資安戰略實驗室(NEITHCyber Security Lab)。結合專業設備與資深人才，得以萃取出最先進且高品質的網路威脅情資。我們的服務範疇以威脅情資為核心，延伸至MDR即時監控、網路流量分析、DNS Security、資安健檢、各式資安事件處理與鑑識服務等，協助客戶防範無所不在的網路威脅。

04-23270003 WWW.NEITHNET.COM info@neithnet.com