

NEITH X

APT威脅偵測防禦系統

經由Netflow收集內部流量，透過取樣、分析與豐富精準的在地化情資比對，進而識別出流量中是否有惡意活動或可疑行為，並在威脅初始階段就提前預警。能集中管控NEITH T 協防節點，讓管理者對網路場域的任何動靜皆一覽無遺，NEITH X將資料分析與即時警報結合，使企業能夠在安全事件發生前，迅速採取預防措施，保障網路環境的完整性。

NEITH X的資安聯防與協作應變能力，能與Windows Active Directory (AD) 系統和事件日誌收集功能無縫連接，能夠迅速偵測到橫向行為異常事件的使用者，並透過NEITH X發現的惡意情資IOC，可即時整合進入防火牆政策，快速進行資安協作應變，加強既有防護設備的能力，中斷駭客Kill Chain攻擊鏈，找出異常行為的使用者，從而提升整體的安全防禦水準。

透過不同維度找出內部可疑行為：

威脅情資指標

NEITH X 定期更新NEITH i 情資，透過比對情資與惡意行為，進行可視化分析，使管理者透過介面快速了解內部網路攻擊樣態。

網路流量行為監控

收集Flow記錄，針對特定網段/IP/時間進行告警監控。

網路行為分析

檢測是否有異常權限行為、DNS惡意網址、非標準網路協定行為。

NEITH X 如何強化企業安全狀態：

檢視資源

依照不同資源區域，進行正規化資源運用，協助企業強化存取控制措施與資安檢查。

行為分析

強化企業資源被不當的測試連線，異常的存取，弱點攻擊等，提供管理者動態調整存取控制原則。

軌跡記錄

執行各資源進行Flow記錄機制，能夠依照紀錄的Flow機制了解各資源連線的目標。

風險管理

提前掌握外部服務的風險資訊，依據存取情境的變更，持續建立各種資安健檢機制。

經由以入侵指標、異常流量、網路行為、風險等級各項指標分析後，在NEITH X中以可視化的圖表，找出內部惡意來源，並可與NEITH T聯防，主動將高風險的連線直接阻絕在外。

採購相關資訊

品項	產品描述及規格說明
<p>NEITH X APT威脅偵測防禦系統 小型流量 (1套/1年授權)</p>	<ul style="list-style-type: none"> ✓ 提供一年免費軟體版本升級 ✓ 提供威脅情資分析模組 ✓ 提供Netflow分析模組 ✓ 包含1套網路威脅收集器 - 1Gbps及1年授權 ✓ 異常活動監控通報
<p>NEITH X APT威脅偵測防禦系統 中型流量 (1套/1年授權)</p>	<ul style="list-style-type: none"> ✓ 提供一年免費軟體版本升級 ✓ 提供威脅情資分析模組 ✓ 提供Netflow分析模組 ✓ 包含2套網路威脅收集器 - 1Gbps及1年授權 ✓ 異常活動監控通報
<p>NEITH X APT威脅偵測防禦系統 大型流量 (1套/1年授權)</p>	<ul style="list-style-type: none"> ✓ 提供一年免費軟體版本升級 ✓ 提供威脅情資分析模組 ✓ 提供Netflow分析模組 ✓ 包含3套網路威脅收集器 - 1Gbps及1年授權 ✓ 異常活動監控通報

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。