Protective DNS的重要性

什麼是Protective DNS(PDNS)

保護性DNS（PDNS）是一種實施政策的遞歸DNS解析器服務，部署在組織網路上游。此服務在通過與一系列已分類的威脅情報比對DNS查詢，以防止向已知惡意域和IP地址的解析，也包含對於查詢記錄或活動內容進行更精細的自動化過濾防護。PDNS支持新興的DNS技術，包括加密的DNS協議支持（DoH/DoT）和IPv6解析。DNS日誌數據將有利於資安團隊大幅提高DNS活動可見性及作爲安全預防政策制定的參考。

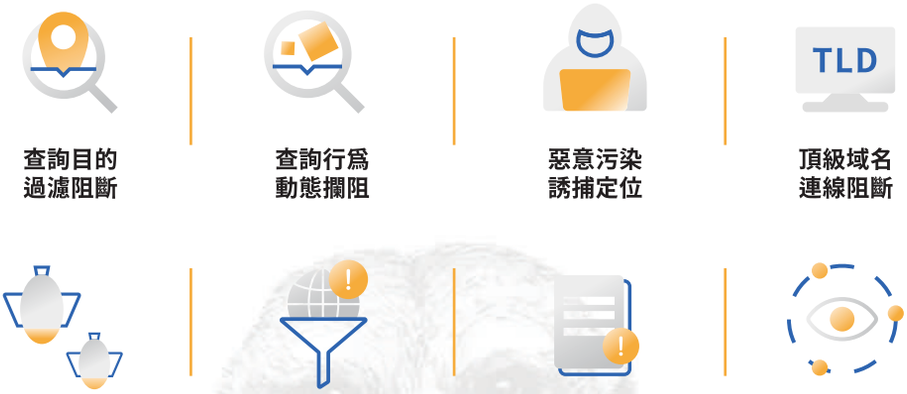
爲何組織需要PDNS

DNS對於組織的OA/OT/IT安全管理整合至關重要。AI技術萌芽後，網路威脅在複雜性和頻率上也不斷演進，傳統的安全措施通常不足以保護敏感數據和基礎設施。PDNS提供了一種積極的防禦機制，用於對抗許多網路威脅，像釣魚攻擊、惡意軟體散播和域名劫持。通過利用先進的算法和威脅情報來源，PDNS賦予組織新能力，能夠在惡意域名造成傷害之前即識別並消除其威脅。此外，PDNS提高了DNS流量的可見性，使組織能夠迅速檢測和緩解基於DNS的攻擊。

台北市中正區忠孝西路一段80號16樓

iSafer在PDNS所扮演角色

iSafer站在資安創新的前沿，提供全面的解決方案，爲企業組織減輕數位風險並保護數據資產。應用PDNS技術進行資安整合時，iSafer增強了安全威脅檢測能力，並加強了對新興網路威脅的防禦措施及敏覺性。利用先進的分析和機器學習算法，iSafer通過提供可視且可執行的活動監管和威脅情報數據，主動識別並預防性地消除惡意活動來滿足PDNS任務。



查詢目的
過濾阻斷

查詢行爲
動態攔阻

惡意污染
誘捕定位

頂級域名
連線阻斷

DNS DDoS
攻擊防護

全球威脅情報
比對過濾

資安風險
指標告示

DNS活動
洞察力

符合法規

iSafer DNS威脅情報及安全亦能擴及應用在SIEM,XDM或NAC等事件管理平臺整合，以符合各產業資安要求如CMMC/NIST800/FISMA/PCI-DSS/HIPAA等，以及ISO/IEC 27001:2022 控制措施認證規範。

Protective DNS是次世代資安防禦必需品

從資安聯防的層面，一個適當的運營和業務恢復策略不僅僅是防止惡意攻擊者進入，還要保護那些可能已經存在內部組織的攻擊者。不幸的是，每個人都會在某個時候受到侵害。在現代資安攻擊的洪流中，威脅行爲者能在企業內部潛伏數周甚至數月而不被察覺，這是許多資安長(CISO)的首要關注。

如果您能在網路殺傷鏈的早期發現異常活動，您將可以在數據外泄和加密之前便使攻擊失效，從而最小化並控制任何損害。早期警報訊號可以讓您在異常升級之前進行調查。

iSafer 是您 PDNS 最佳解決方案

www.urmazi.com

台北市中正區忠孝西路一段80號16樓
SF-WP-40319