Datasheet

ThreatReveal

TEAMT5

ThreatReveal

威脅情資風險識別平台

洞察潛藏風險
看清切身威脅

企業外部資產潛藏的安全弱點，可能在資安團隊察覺風險前，就成為攻擊者進入系統或存取資料的途徑。傳統漏洞掃描能協助找出系統中的安全弱點，但僅從漏洞狀態，無法判斷漏洞是否已遭利用。這項差異至關重要：可能遭利用的漏洞，與已出現入侵跡象的系統，需要採取的應對方式並不相同。

為什麼選擇 ThreatReveal？

TeamT5 威脅研究團隊分析攻擊者如何利用漏洞，以及攻擊者留下的痕跡與行為，並將研究成果轉化為偵測規則。ThreatReveal 將這些規則應用於可從外部存取的系統，協助團隊區分潛在風險與可能顯示已遭入侵的跡象，進一步判斷後續應進行修補或深入調查。

核心功能

掌握外部可存取資產

盤點關聯子網域、IP 位址、開放連接埠、可從外部存取的服務與偵測到的技術資訊，協助掌握哪些資產與服務可能潛藏風險。

發現外部安全弱點與不應公開的資訊

找出漏洞、不安全設定與存取控制缺失，以及不應公開存取的機敏資訊。

辨識入侵跡象

運用 TeamT5 自研偵測規則，辨識攻擊者留下的線索，找出漏洞可能已遭成功利用或未經授權存取的跡象。

聚焦關鍵風險提供處置方向

ThreatReveal 綜合嚴重度、曝險時間與風險脈絡，協助團隊排定風險項目的處理優先順序；同時提供技術證據與修補建議，以利確認風險、採取後續處置，並判斷哪些項目需要進一步調查。

ThreatReveal 風險識別面向

ThreatReveal 可識別的風險涵蓋以下五大面向：

類別	可協助釐清的風險
網路應用程式安全	掌握網路應用程式中可能讓攻擊者進入系統或存取資料途徑的風險
系統與服務設定	找出可能讓系統更容易遭存取或濫用的對外服務與不安全設定
資訊與資料保護	找出不應公開於網際網路的機敏資訊
網域與基礎設施	識別網域及相關基礎設施可能遭濫用的風險
入侵跡象	透過外部可觀察到的證據，判斷是否需要進一步調查

說明：風險識別結果反映納入範圍的網域與 IP 位址，以及掃描當下可觀察到的狀態。隨著基礎設施變動，資產、服務與漏洞狀態亦可能改變。

ThreatReveal 適用情境

盤點外部資產情況	掌握需優先處理的關鍵風險	調查疑似入侵的跡象
了解哪些資產、服務與技術資訊可從外部觸及，並確認哪些項目需要由內部進一步檢視或追蹤。	聚焦持續存在或風險較高的安全弱點，排定修補優先順序。	運用 ThreatReveal 辨識入侵跡象與相關技術證據，判斷哪些風險項目除了例行修補之外，還需要進一步調查。



關於 TeamT5

v.202609

廣受全球 550 家以上客戶信賴，橫跨政府單位、科技、製造、金融、醫療、軍事、電信等產業。

頂尖專家團隊

團隊成員常在世界級資安會議中發表最新頂尖研究，包含臺灣 HITCON、美國 Black Hat、日本 Code Blue / AVTOKYO、德國 Troopers，及國際組織辦理的 Hack In The Box 與 FIRST，於威脅情資研究與資安先進技術領域擁有世界領先地位。

外界肯定

獲得美國 Bloomberg 及 CNN、日本產經新聞及朝日新聞、韓國 ET News 等採訪報導。更於 2022 年獲得日本三大巨頭投資，包含日本最大創投 JAFCO 集富集團、日本最大跨國企業並在全球皆有商業投資的 ITOCHU 伊藤忠商事，與日本最大資安解決方案提供商 MACNICA。

Tel 02-7706-1299
E-mail sales@teamt5.org

TEAMT5 | THREAT INTELLIGENCE PIONEER, BORN IN ASIA