

技術詞彙表

本技術詞彙表載有本文件所用與本公司及我們業務有關的若干技術詞彙的解釋。該等術語及其涵義未必與業內所採用的標準涵義或用法一致。

「對抗樣本變異引擎」	指	利用受控變異技術自動生成及修改攻擊輸入(對抗樣本)以測試、規避或加強檢測模型的系統。
「AI」	指	人工智能。
「AIoT」	指	人工智能物聯網。
「API」	指	應用程序編程接口，係允許不同應用程式或系統間相互通信、調用功能與交換數據之軟件中介。
「行為建模」	指	分析及學習用戶、系統或網絡中正常及異常活動模式以檢測可能顯示惡意行為的偏差之過程。
「容器」	指	一種輕量級且具隔離性的運行環境，將應用程序及其依賴項打包，同時共享主機操作系統內核。
「數據外洩」	指	數據被故意或意外地洩露、傳輸、訪問或披露給未授權的個人、組織或系統的行為，包括蓄意竊取和誤操作、系統漏洞導致的意外洩露。
「數據盤點」	指	組織數據資產的系統化記錄，包括其存放位置、類型、所有權及敏感度。
「數據譜系」	指	對數據由其源頭起跨系統的所有轉換及流轉的追蹤。
「數據駐留」	指	數據存儲及處理的地理位置及司法管轄區域。
「脫敏」	指	通過技術手段對敏感數據進行轉換、遮蔽或替換，以防止未經授權的訪問和洩露，同時在特定場景下保持數據的可用性。
「同態加密」	指	一種允許於不解密的情況下直接對加密數據進行計算的密碼學技術。
「信息孤島」	指	組織內部相互獨立、難以互通、共享或整合之孤立數據系統或存儲庫。
「IoT」	指	物聯網

技術詞彙表

「日誌」	指	由系統、應用程序或設備產生的事件或活動記錄。
「機器學習」	指	一種使系統能夠從數據中學習模式及提升效能而無需進行明確編程的方法。
「掩碼」	指	數據脫敏的常用技術之一，通過部分隱藏數據內容實現脫敏。
「元數據」	指	用於描述、標註或解釋其他數據之屬性、來源、結構、使用方式與上下文信息之數據。
「滲透測試」	指	授權的安全專業人員模擬真實攻擊者的技術和方法，對目標系統、網絡或應用進行攻擊性測試，以主動發現安全漏洞、評估安全風險並驗證現有防護措施有效性的過程。
「拍字節」	指	一種數據計量單位，1拍字節(PB)等於1,024太字節(TB)，1太字節等於1,024吉字節(GB)。
「權限提升」	指	利用系統漏洞以獲取高於其初始授予權限的存取權限。
「紅藍對抗」	指	一種由攻擊方(紅隊)與防禦方(藍隊)模擬真實世界的威脅以測試及提升安全能力的網絡安全演練。
「保留規則」	指	界定數據存儲期限以及何時應將其歸檔或刪除的規則。
「安全數據中心」	指	一個用於存儲、管理及保護數據且整合實體及數據安全控制措施的集中式設施或系統。
「SOAR」	指	安全編排、自動化與響應，為一種整合多種工具並實現工作流程自動化以高效檢測、分析及響應安全威脅的網絡安全方法。
「SQL」	指	結構化查詢語言，為一種用於管理及查詢存儲於關係型數據庫中的數據的編程語言。
「壓力測試」	指	評估一個系統於極端或高負載條件下的性能及韌性的過程。
「威脅情報」	指	有關潛在或現有網絡威脅的資料及分析，用於為安全決策提供依據並加以改進。
「虛擬化」	指	透過對硬件資源進行抽象化，使多個隔離的計算環境得以於單一物理系統上運行的技術。