Web X-RAY

雲 端 網 頁 側 錄 系 統 WEB X-RAY™

WEB X-RAY™ 是一個網站伺服器的監視側錄器。其主要功能就像是常見的監視器或是行車記錄器一般，可長時間即時側錄相關的資訊。WEB X-RAY™側錄整個網站交易資料的輸入及輸出，可隨時調閱並即時偵測來自企業內外部的攻擊與通知，實戰的攻防經驗豐富且可驗證結果，是資安鑑識與防禦的最佳利器。

轟動全國第一銀行八千萬盜領案，駭客如電影情節般令 ATM 自動吐鈔的誇張方式搬走現金，手法令人大開眼界，資安議題的重要性再度被搬上檯面。這個案件雖然警方最後靠著密佈整個台灣路口的監視器循線逮人抓到了嫌犯。然而破案至今，檢調依舊無法得知駭客的入侵手法，甚至查無任何入侵的蛛絲馬跡，真是讓人感到驚訝。如果不能發現真正的問題所在並進而解決，難保不會有下一次的攻擊從相同的漏洞再次攻進來。

路口有監視器，警方要找人，這就很重要。開車有行車記錄器，撞了車要還原現場釐清責任就知道很重要，這類的監視裝置，都是用來記錄完整過程的工具，可調閱關鍵畫面，但是我們用來營運的網站可有監視器? 沒有監視器，網站在傳送甚麼資料出去，你可知道? 可有記錄供調閱? 可有警示機制? 國內高科技公司三度被駭客從海外分公司一路攻擊到總部並竊取資料公布。該公司有專業資安服務子公司，而駭客能避開所有偵測機制從容不迫的攻擊成功並帶走資料，顯示目前的資安設備對偵測駭客攻擊已經力有未逮。

網站伺服器具有 365 天，每天 24 小時不停機的服務特性，不僅是企業提供服務的最佳利器，同時這樣的特性也是駭客攻擊的首選目標，只要被發現漏洞，駭客能在極短的時間內攻入系統，在你真正抓到入侵者之前，這是一個可以提供全年無休服務的接入點，不可不慎。

WEB X-RAY™ : 解密駭客的攻擊過程。

在 WEB X-RAY™ 推出之前，網站伺服器的運作猶如黑盒子，到底網站送出哪些資料，無法知曉，即便使用 Sniffer 也只能記錄一小段時間。而測試僅僅能針對正常的網頁存取，對於駭客如何利用網站伺服器來擷取資料或是下達攻擊指令則是一無所悉。企業對外服務網站無論任何原因停止服務，對業務與形象都有不可承受的龐大壓力。當發生問題，無論是資安事件或系統錯誤，**能不能在最短時間內偵測並找到真正問題點之所在，及時解決，才是整個事件中最困難的部分**。而有無記錄，則是其中的關鍵點。眼見為憑，就像監視器一樣，有記錄，就能找人或是找問題，沒記錄，就只能憑剩餘的蛛絲馬跡如 CSI 般的慢慢拼湊還原現場了，而事實上，駭客為了避免被追蹤，會盡其所能刪除所有系統記錄檔與軌跡，因此大部分的情況是無法還原，而就算是請了資安專家花時間勾稽相關記錄來嘗試還原過程，其實也不能肯定就是真正的過程，因為現場已經消失了，所能拼湊的也就是推論的結果。只有錄下，才能真正還原，就像我們看監視器記錄一樣，看到畫面了，無須描述就能理解了。

小松鼠軟體針對這樣的問題及需求推出一個高效能，全方位側錄、偵測攻擊且穩定易於管理的資安鑑識工具: WEB X-RAY™。這是首見於市面的可長時間側錄網站伺服器的系統，猶如一個 X 光機般，讓網站的所有運作細節照的一覽無遺，無論是偵測駭客攻擊、內部員工存取管理、事後的稽核及損害控管，一次幫客戶完成這幾件最重要的事。W3C 的記錄只能告訴你誰來過網站，卻不能告訴正確的告訴你來過的人到底做了甚麼，是真正的交易? 還是攻擊? WEB X-RAY™ 則可以達成以上的目的，透過交互查詢，更能完整側寫整個駭客的攻擊過程與細節。WEB X-RAY™絕對是企業網站運作不可缺少的必備系統。

WEB X-RAY™企業版產品功能表	
網頁伺服器記錄	網頁存取紀錄，含網頁執行時間等相關細節。
	HTTP 200 網頁輸出記錄。
	HTTP 200 使用記錄、軌跡資料及證據保存。
	攻擊偵測紀錄。
	HTTP 500 錯誤畫面記錄。
	HTTP 500 錯誤訊息可提供系統開發者重要訊息供開發者修正程式，提高系統穩定度。
稽核及損害控制	檢查非法連結及其來源：可檢視詳細非法連結來源及其網址，所傳送之攻擊指令等細節。
	輸出網頁內容條件檢索。
安全	支援 SSL, HTTP/2 及 TLS1.2/TLS1.3 資料傳輸使用 AES 256 及 RSA 2048/4096bit 加密運算。
	HTTP XML Web Service 防護：保護 xml web service 避免未授權網址存取 XML Web Service API。
	依照用戶端國家來源阻擋網頁服務，免受特定國家網路使用者攻擊，可提供二次驗證機制(此為客製化整合項目)。
效能	支援 IPv4 及 IPv6。
	高效能規則引擎，高效能模組，支援關鍵字及 regular expression 正則表示法過濾規則。
	網頁監視伺服器支援 MySQL。
	高效能資料查詢介面。
	擴充性(Scalability)：分散式架構，企業版可大量橫向擴充(scale out)網頁伺服器。
網頁攻擊偵測	HighBit Shell Code 偵測。
	Parent Path 偵測。
	Directory Traversal 偵測。
	Hex Encoding 偵測。
	SQL Injection、XSS(Cross Site Scripting)、CSRF(Cross-Site Request Forgery) 偵測。
	即時 Email 警示訊息通知。
	WAF 模組(選購)
	白名單(White List)設定。起始網址(Start URL)設定。拒絕網址(Deny URL)設定。
	HTTP Header 偵測防護。
	根據 URL 自訂防禦與偵測規則(Per URL rule support)。
	自訂輸入特徵檢查規則(Input Pattern Rule)。
	掃描 POST 資料。
	掃描 GET 資料 (URL Scan)。
支援平台	支援作業系統與版本： 本機安裝支援: Linux CentOS 7 Apache 2.4, Amazon Linux AMI Apache 2.4，Ubuntu 20.04 LTS Apache，Windows IIS 7.0(含)以上 Windows 2012/2016/2019/2022 x64，Nginx (1.18 以上，需洽詢後方能支援)。 Reverse Proxy Mode: WEB X-RAY™ 使用 Reverse Proxy Mode，後端防護之 Web Server 無版本及系統限制。 企業版記錄空間上限 5TB。XRAY 可記錄資料量 64TB，如需更多記錄資料可另行洽談規劃不受上限影響。

TSM Software 小松鼠軟體

TSM Software Technology, Inc.
小松鼠軟體有限公司
新北市中和區景平路 288 號 13 樓之 15
Tel: +886-2-2941-5500
http://www.tsmst.com