Cyber Security Solutions

Managed Detection & Response Solutions

駭客平均潛伏時間500天 資安防禦概念要轉型

在早期的資安防禦策略中，主要利用縱深防禦。透過層層構築不同防禦機制，以期增加駭客入侵難度，最終逼迫攻擊者放棄繼續入侵的意願。但是近年來APT這樣的風險，已經讓透過增加入侵難度，使得攻擊者放棄攻擊的情況，幾乎不是可行方法。根據趨勢科技過往揭露的臺灣企業平均遭駭客潛伏的時間，已經到達598天(資料來源：https://www.ithome.com.tw/news/108118)，這樣的驚人數據。這個數據代表著是駭客將會不計時間成本，只為成功入侵後取得的驚人利益。背後的意義更代表著，即便駭客已經入侵到組織內部，可以進行各種活動，而組織仍然需要超過500天的時間才能發現。如果經歷一段這麼長的時間，卻沒有任何辦法可以發現攻擊者的足跡，那麼在500多天的時間內，要偷取到組織的機密資料或金錢，是非常有可能辦到的事。

這是現在所有組織面臨到資安最大的問題，攻擊者被實際上的金錢利益吸引，攻擊可能發生在任何組織，只要攻擊者有意願，攻擊隨時可能發生。

令人最沮喪的部分則是，幾乎所有人都會選擇在門口(網路出口端)部署層層重兵(各式資安設備)防守，但在沒有100%的偵測率的情況下，必然會有少數攻擊會成功入侵到內部。然後攻擊者平均有500多天的時間，可以在內部網路逛大街。如果還用傳統的防禦策略面對現有的威脅模式，那麼被攻擊成功並發生損失，似乎也是必然的結果。因此，我們必須正視現在的資安威脅，並採取更積極的手段來控制損失。從現在開始的資安防禦概念勢必要轉型，當我們可以認知沒有任何資安設備可以100%偵測到攻擊，那麼被攻擊成功的機率就變成100%。但仔細審視所有資安事件的報告，我們可以發現，攻擊者從發動攻擊，到真正取得不法利益，是需要時間來辦到，而這時間往往從數個月到數年。但是在傳統的防禦機制下，我們全力將防禦機制都放在網路的出入口，卻沒有任何辦法，去處理攻擊者在內部開始的活動。一次潛伏期為一年的攻擊，代表著你在一年時間內，只要發現任何一個蛛絲馬跡，這次的攻擊可能就被消彌。但是每一次的資安事件新聞不停的停醒著我們，面對突破大門以後的入侵過程，我們幾乎毫無招架之力。

資安設備無法達到 100% 防禦 MDR 服務更顯重要

面對攻擊者在資訊安全上的威脅，我們無一不期待能有個終極解決方案。只要使用這個終極解決方案，就再也不用擔心資安的威脅。這是一個美夢，但是現實是，目前所有的資安設備都做不到100%的偵測率。在這個前提下，當防禦架構是建置層層的資安防護設備，其實就代表資安事件還是可能會發生。偏偏現在主流大部分的防禦架構都是阻擋在網路的出口端，或是部分網路的集中處。當攻擊者成功躲過閘道端的設備，後續要進行處理就變得非常困難。

對比傳統的資安防禦策略或觀念，先從各式自動化偵測入侵風險的設備開始。當建設到一定數量的資安防護設備後，考慮到管理與後續處理的效率，很多組織會開始導入SIEM這種類型的方案，透過集中收集每個資安設備的紀錄，再加上SIEM本身的關聯分析，以求可以做到集中管理與分析資安風險的目標。我國也有多家資安服務廠商，提供委外使用的SIEM服務，就是市場上可以找到的SOC廠商。依據我國的政策管理辦法，在政府與金融有著比較明確的規範，所以SIEM這種解決方案的採用者，主要也出現於政府與金融產業。我國的SOC廠商，皆提供符合政策規範的相關功能，例如：提供一定年限的紀錄保存功能，或是收集資安設備警訊定關聯後，發出對應的資安事件通報。但關於後續協助處理的機制，往往就比較缺乏，大多需要依賴使用者自行處理。我國SOC目前提供的服務在Gartner的定義中，屬於MSS(Managed Security Services)。但在2017年5月，Gartner 發布一份新的市場指南，提到更 新一代的 MDR (Managed Detection and Response) 強調持續性的威脅偵測與監控機制，同時提供客戶完善的資安事件處理能力。讓使用者不需要對於排山倒海而來的大量警報疲於奔命。透過MDR軟體服務提供偵測、分析及處理一次到位的服務方案。

產品特色

平台功能

即時檢測端點威脅

資安攻擊日趨"針對性"　及"持續性",越來越多的攻擊可繞過傳統的資安設備防線,直達端點

軟體授權

持續性的檢測 監控及分析

傳統一次性或定期檢測方式,常出現"時間差"及"漏網之魚"等問題,沒辦法在事件發生擴大前即時發現或阻斷,更無法進行追蹤

資安事件回應及遠端處理

資安事件具"時效性" 及"迫切性",需在災損出現或擴大前予以及時處理.

管理偵測回應(MDR)中央管理平台軟體一年授權
管理偵測回應(MDR)軟體(5U,10U,50U,100U) 一年授權

ENDBLOCK BLOCK ALL ENDPOINT THREATS
耘通科技股份有限公司 Cloudhood Technology Corporation
台北市信義區松山路130號10樓之1 T：02-2712-0855 F：02-2756-5785 M：Gary@cloudhood.com.tw