Cyberint
全方位攻擊面監控技術

Cyberint

> “Cyberint 團隊總讓我有一種信任感，在我需要時隨時都會為我提供協助。他們總是能提供支援的這種感覺是無價的，有自信提供我們足夠的資安能見度，也能主動應對各種不同的網路威脅。”

GCash 資安長
Mark Frogoso

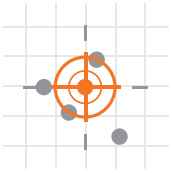
有漏洞可利用的連接埠、暴露在外的公司網路介面、可被攔截的子網域及 SSL/TLS 問題等，這些只是企業組織不斷擴大的攻擊面數量中所面臨的少數威脅而已。

企業組織會進行反制，但是這通常會導致安全團隊從不同方向進行工作；這意味著多重解決方案只會產生單一的告警。

Cyberint 全面整合性的方法和其它解決方案有所不同，因為它結合了外部攻擊面監控 (Attack Surface Monitoring, ASM) 和進階的威脅情資。這兩個模組以緊密協作的方式持續地注入並強化 Argos Edge™，以提供全方位的解決方案，可用於持續發現資產、監控並識別風險，以及協助進行補救。

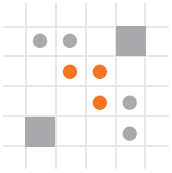
攻擊面監控功能 - 識別其它解決方案無法做到的弱點和漏洞。

Argos Edge™ 攻擊面監控
保護您不受外部威脅的方法



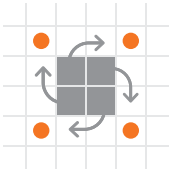
全面整合的解決方案

藉由結合 Argos Edge™ 攻擊面監控和進階威脅情資平台的方法，取得對您數位資產全面性且自動化的能見度。



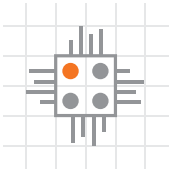
靈活且具有彈性的數位風險防護 (DRP)

首先從識別和監控您企業組織的攻擊面來著手。擴大因應與其它數位風險防護 (Digital Risk Protection, DRP) 相關的挑戰，隨著您安全性逐漸成熟的各個階段不斷發展。



進階的資產偵測和準確的資產歸因

持續偵測並準確監控歸屬公司的各種資產類型，以識別未知的資產和隱形 IT (Shadow IT)。



AI 驅動的簡易性

利用我們以 AI 驅動的技術來即時取得可採取行動、重點性的相關告警，以因應複雜的安全性挑戰。

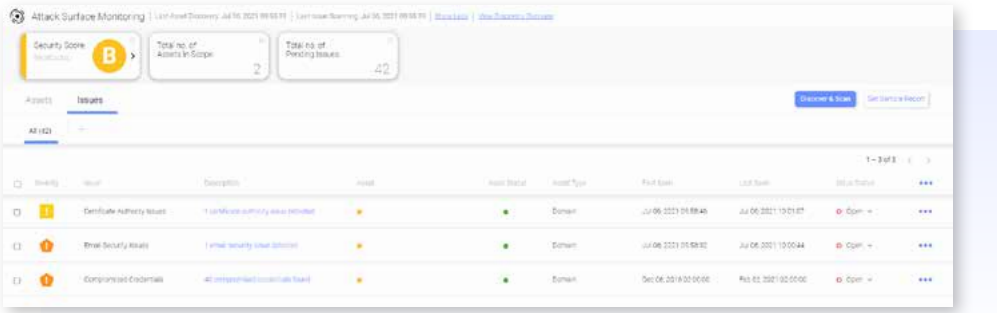
全面範圍涵蓋和操作管控

利用 Argos Edge™ 攻擊面監控的兩個關鍵性組件來控管您在數位環境中的活動。

偵測與掃描

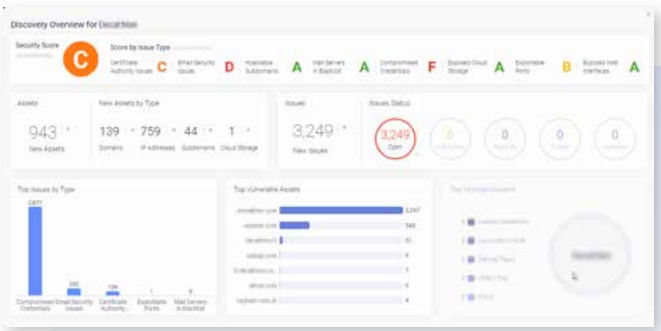
持續偵測並對應所有外部的資產。掃描威脅危害您企業組織的問題和漏洞。

- 將偵測數位資產的功能自動化
- 將您企業組織的數位活動作定期重新對應的設定，以重新驗證並更新資產
- 識別關鍵性的資產並將其作分類
- 識別不再附屬於公司的資產和新的資產
- 啟動您數位活動的歷史紀錄追蹤



管理

調整所有發現的資產並依重要性作優先排序，以能達到最理想的處置和管理。持續監控新的問題。



- 追蹤問題從偵測到解決的生命週期
- 計算安全分數以評估風險並將其依重要性作優先排序
- 自動將已解決的問題進行結案
- 就問題處理方面啟動歷史紀錄的快照 (Snapshot)
- 包括臨時和定期報告的報告功能

Argos Edge™ 攻擊面監控的運作方式

從自動化的偵測，到管理即時問題並提供安全風險計分，各大產業的主要企業組織皆選擇 Cyberint 作為其攻擊面監控的解決方案。

偵測

Step 1

揭露和對應

揭露您的數位活動，並對應所有外部的數位資產。這包括網域、子網域、雲端儲存等等。Argos Edge™ 是 Cyberint 專屬的平台，能從多個開放式、深網和暗網資料來源收集資訊，以作為揭露您企業組織數位活動的全面性方法，而且還讓您可以偵測到隱形 IT。

Step 2

掃描和偵測

掃描並偵測出貴公司數位活動中的問題和漏洞，例如洩漏的憑證、惡意軟體的感染、有漏洞可利用的開放式連接埠、有漏洞的網路介面等等。 Cyberint 主控台能以精細化的操作檢視畫面顯示所有的資產和問題。

Step 3

評估風險

將目前的威脅與您企業組織目前的最佳實務及其目前管理問題的方式做比較，藉以計算安全分數。考慮情境並評估安全分數，就更能隨時評估您企業組織面臨的風險。

管理

Step 4

監控和重作

依優先順序對所有發現的資產和問題採取行動。在操作檢視畫面中將其提報給您的安全團隊，以便處理、管理問題狀態和分配，以及資產管理。移除並加入資產，同時並針對最具關鍵性的資產設定不同的優先處理順序。

Step 5

依優先順序採取行動

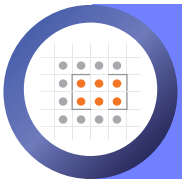
持續性的識別映射該企業組織的資產，藉以發現新的資產，並對識別出來的任何漏洞或威脅採取行動。

Argos Edge™ 攻擊面監控能將廣泛的各種外部威脅依優先順序進行處理

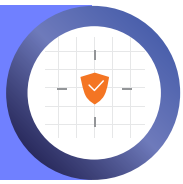
可利用的連接埠

在攻擊者發現之前偵測出潛在性可利用的連接埠，並避免敏感資訊的洩漏或內部系統的存取。識別出暴露的應用程式，以防攻擊者用來竊取私有和受管控的資料。

暴露的公司網路介面



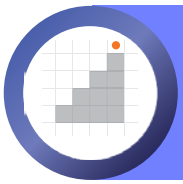
持續監控並掃描暴露的網路介面，因為威脅者可利用洩漏的敏感性資訊。若有第三方技術具有與您企業組織數位活動介接的已知漏洞，即會被自動偵測。



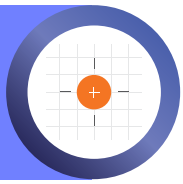
電子郵件的安全問題

追蹤並管理電子郵件驗證標準的不當設定。防範可在您網路中傳播惡意軟體並存取內部資訊的網路釣魚攻擊（Phishing）活動。防禦針對客戶的網路釣魚攻擊活動，因為該攻擊活動會導致客戶流失並損害品牌聲譽。

憑證頒發機構授權 (CERTIFICATION AUTHORITY AUTHORIZATION, CAA)



監控憑證授權標準的不當設定，因為該情況會使威脅參與者得以對非法網站發佈合法憑證。識別出因此而產生的風險，因為威脅參與者會利用網域間的信任關係來執行網路釣魚攻擊活動。

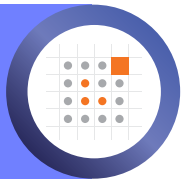


列入黑名單的郵件伺服器

發現 DNSBL 伺服器黑名單儲存庫中所列的 IP 位址。識別因可疑或垃圾郵件活動而被標記的 IP 位址。

可劫持的子網域

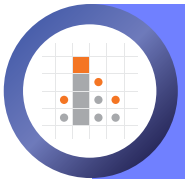
持續發現已經或可能被劫持的子網域。該子網域可能會被用來對您的企業組織和客戶進行複雜的網路釣魚攻擊。在任何使用易受攻擊的網域服務中，此類攻擊會擴展至登入使用者被攔截的會話 (Session)。



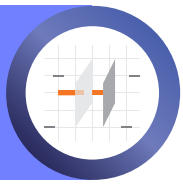
開放式的雲端儲存

追蹤並持續更新您對暴露的雲端儲存帳戶的監控。防範威脅參與者修改您的資料並注入惡意的內容，進而對您包括員工、客戶、合作夥伴和系統在內的整個企業組織造成風險。

遭竊的身分憑證



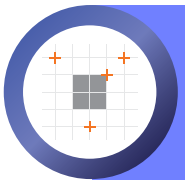
保護您員工和客戶在暗網上的憑證，因為惡意參與者會用以試圖取得內部資料的存取權限。本模組可防範非法存取網路服務，以對關鍵員工執行魚叉式網路釣魚 (Spear Phishing) 攻擊，進而獲得整個企業組織系統的存取權限。



SSL/TLS 問題

為您的企業組織做好防護，使其不致因為有漏洞而被遭受薄弱的加密套件 (Cipher Suite)、金鑰等的各種攻擊。此類攻擊有可能會造成流量攔截 (Traffic Interception) 或資料交換解密，使中間人攻擊 (Man-in-the-Middle Attack) 得以冒充伺服器，或洩漏來自用戶端和伺服器之間通訊的資料。

網頁應用程式安全問題



識別安全性標頭 (Security Header) 的不當設定。此不當設定會使您的企業組織無法抵禦中間人攻擊、跨網站指令碼 (Cross-site Scripting)、資料損壞、敏感性資料的暴露和各種攻擊。

關於 Cyberint

Cyberint 相信藉由為客戶提供防護，使其免受外部網路攻擊，能使網路世界成為一個更安全的地方。我們實現此點的方式是利用專家知識和威脅情資提供一套豐富的、自動化且量身訂做的智能數位風險防護解決方案。 **Cyberint** 為全球各地的領導品牌提供服務，其中包括橫跨如金融、零售、醫療保健、電子商務、遊戲、媒體等產業的財星美國 **500 (Fortune 500)** 大公司。

Contact information:

橙鎵科技股份有限公司

Tel: 02-8751 5663 Mail: sales@ortech.com.tw
Fax: 02-8751 5680 114 台北市內湖區瑞光路583巷25號3F