智能數位資產風險防護

Cyberint

ABP
安普新科技

saletw@abpsecurite.com
+886-2-2740-7198
台北市中山區南京東路三段 208 號 9 樓

智能數位資產風險防護

Cyberint 充分運用獨特的 Argos™ 組合，即專業的威脅情報平台和經驗豐富的威脅情報分析師，藉以提供全新的數位資產保障 (Digital Risk Protection, DRP)方法，專為因應以下的挑戰而提供解決方案：

- 決定應納入考量的相關威脅，以設計出有效的網路安全防禦計劃
- 透過明確的行動計劃向董事會和管理層說明最新的網路風險狀況
- 取得預測性的情報，以識別出意圖、手法和工具，藉此在目標威脅發生前加以緩解
- 持續監控網路犯罪分子可能利用的數位風險漏洞
- 檢測違規並傳播到組織外部的惡意情資
- 了解在外不斷發展，而且鎖定您的品牌和客戶為目標的網路攻擊

CYBERINT 能協助您因應的商業挑戰：

- **品牌形象保護**
- **協力廠商的網路風險**
- **數位資產風險面的監控**
- **網路詐欺**
- **資料洩漏偵測**
- **資安意識 (Attackware) 偵測**
- **暗網 (Dark Web) 監控**
- **威脅情資**

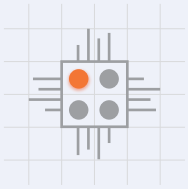
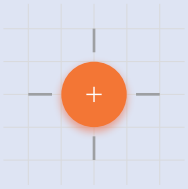
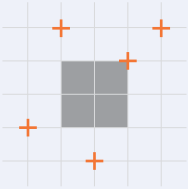
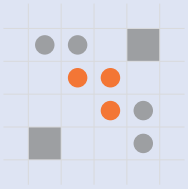
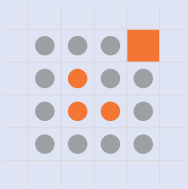
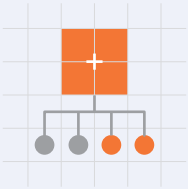
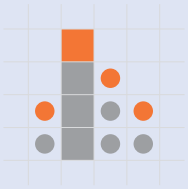
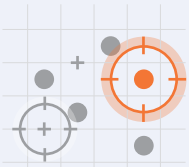
Gartner peerinsights™ **4.8** ★★★★

> **這是一項可將發現的結果轉化成為我們企業量身訂做的相關資訊和告警，從而提供真正的價值的託管服務。**

> **您要在使用 Cyberint 之後，才會真正了解試圖攻擊您企業組織的對象是誰**

saletw@abpsecurite.com +886-2-2740-7198 台北市中山區南京東路三段 208 號 9 樓

CYBERINT OFFERING

ARGOS™ TECHNOLOGY	MANAGED SERVICE
 威脅情資	 目標監控
 暗網監控	 智能人力情報
 攻擊面拼湊	 深入調查
 鑑識資料視覺化	 威脅情資蒐集和分析
 偽冒網站偵測及下架	

saletw@abpsecurite.com +886-2-2740-7198 台北市中山區南京東路三段 208 號 9 樓

ARGOS™ 智能數位資產風險防護平台

Argos™ 是一個多租戶且具有數個模組的 SaaS 平台，其中包括：

攻擊面拼湊 (Attack Surface Mapping)

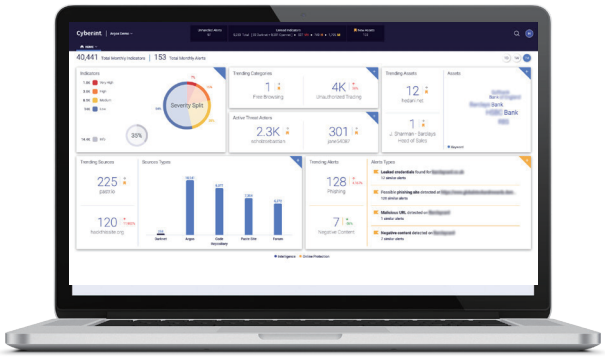
Argos™ 攻擊面拼湊模組可識別企業組織的數位足跡 (Digital Footprint)，並持續監控外圍的資產，以確保提供該資產的能見度，方法是依據嚴重性將要處理的問題以優先順序排列，從而突顯出相關的威脅、漏洞和弱點。

Argos™ Digital Risk Protection Platform, Attack Surface Monitoring

威脅情資蒐集和分析

Cyberint 能即時監控開放網路、深網 (Deep Web) 和暗網中成千上萬個威脅來源，因此每天能向 Argos™ 的內部資料網 (Data Lake) 蒐集數以百萬計的情資項目。

原始情資項目會自動與企業組織的資產 (包括 IP、網域、品牌、主管等等) 相互關聯，並根據特定的使用個案進行分類，範疇包括釣魚網站 (Phishing)、惡意軟體活動、憑證填充 (Credential Stuffing)、資料洩漏、欺詐活動等等。利用 Cyberint 專業的機器學習演算法，可根據潛在風險和影響對此原始情資依優先順序排列，進而提供智慧型且具成本效益的分析。

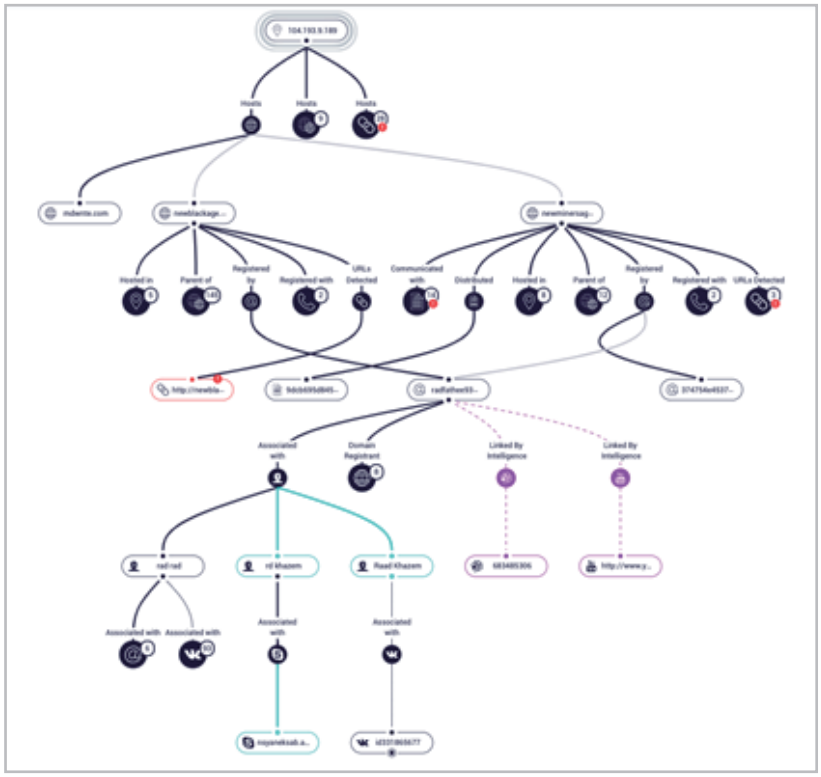


Argos™ Digital Risk Protection Platform

自動化和半自動化的分析引擎會建立可採取行動的告警，然後透過深入的分析、豐富的背景信息、威脅參與者分析等向資安團隊發出告警，讓企業組織能採取有效的行動。

saletw@abpsecurite.com +886-2-2740-7198 台北市中山區南京東路三段 208 號 9 樓

鑑識資料視覺化 (Forensic Canvas)



Argos™ Digital Risk Protection Platform, Forensic Canvas

Cyberint 的鑑識資料視覺化模組能識別及分析威脅參與者，並深入調查他們使用的工具、戰術和流程 (TTPs; Tools, Tactics and Procedures)。

鑑識資料視覺化模組的利用有助於使特定或多個入侵指標 (IOC) 的背景信息更加充實，進而將多項服務整合成統一的調查平台，以支援各種連線，包括 Argos™ 威脅情資、WHOIS 服務、被動域名系統(DNS)、社交探索(Social Discovery)、惡意程式碼偵測等等。

主動式釣魚網站 (Phishing) 偵測技術及偽冒網站下架 (Takedown)

釣魚網站仍然是數位企業組織的主要風險。此類攻擊不僅造成帳戶被接管、客戶流失，而且還會對品牌聲譽造成負面的影響。

為因應此一挑戰，Cyberint 開發出釣魚網站信標 (Phishing Beacon)。它是一個專業的模組，能即時查看仿冒企業組織網站內容建立而成的新釣魚網站。這是威脅參與者所利用的一種有效的技術。Cyberint 的迅速偵測讓我們能代表企業組織將釣魚網站撤下，以快速消除風險。

為您帶來的效益

- 降低Shadow IT 的安全性風險
- 深入了解您的網路攻擊面
- 縮短威脅停留的時間
- 擴展您的團隊能力
- 降低網路安全的總擁有成本 (TCO)

saletw@abpsecurite.com +886-2-2740-7198 台北市中山區南京東路三段 208 號 9 樓

託管服務

針對您的需求量身訂做的網路情資服務

強化威脅情資團隊

Cyberint 提供託管的數位資產風險防護 (Digital Risk Protection) 計畫，讓您能使用我們的 Argos™ 平台和網路威脅分析師團隊，藉此提高任何網路威脅情資 (CTI) 計畫的品質和效能。

Cyberint 的分析師團隊每天會與您內部團隊成員的專職分析師互動。分析師是根據其產業知識和對業務需求的深入了解來分派的。

Argos™ 揭露的所有原始情資項目都經過認真的驗證和背景化，並利用從開放式網路、深網和暗網蒐集的大量資料來歸因於真正的風險。

我們的分析師團隊會講多國語言，因此可以用他們各自的語言來了解威脅參與者。此外，分析師對網路犯罪「術語」和文化的掌握讓您能夠識別、驗證和減緩很有可能成為攻擊的威脅。

Cyberint 在研究、調查和威脅情資作業方面提供寶貴的人為因素。臥底情資 (Virtual HUMINT) 功能，即與威脅參與者的實時互動，在有效減緩威脅方面有必要時可達到更深入的背景化。

CYBERINT 研究

Cyberint 的網路研究團隊 (Cyber Research Team) 探索網路威脅的新領域，以在策略上持續了解趨勢性的威脅。該網路研究團隊分析大量的資料，以建立策略性的威脅情資報告，讓決策制定者能夠識別有意義的趨勢，並在以其企業組織為目標的數位資產風險方面有更廣泛和更深入的看法。該報告包括對目前行業風險、值得注意的威脅參與者、工具、戰術和流程 (TTP) 分析等的定期分析。

CYBERINT 最新報告

菲律賓金融業
威脅形勢報告

DOWNLOAD

REvil - 竊取、加密和
拍賣研究報告

DOWNLOAD

在台灣鎖定為目標的勒索
軟體攻擊研究報告

DOWNLOAD

saletw@abpsecurite.com +886-2-2740-7198 台北市中山區南京東路三段 208 號 9 樓

與 CYBERINT 託管威脅情資服務合作的效益

威脅偵測

利用預測性情資偵測威脅

識別嚴重性

識別威脅的嚴重性並了解「大局」

臥底情資 (VIRTUAL HUMINT)

直接與威脅參與者互動、將其行動歸因於特定的活動，並取得更多的背景信息和情資

識別欺詐行為

識別並提供如何回應和減緩威脅的情資，以供採取行動之用

釣魚網站 (Phishing) 的即時偵測

即時偵測出釣魚網站並將其撤下的作業

重要人物的威脅調查

監控您企業核心人物在線上的狀態，以防止威脅參與者取得個人資訊並用來從事惡意活動

拼湊和監控

拼湊出企業組織存在的數位資產並對其進行監控，包括憑證洩漏、數位資產的弱點及敏感性的文件洩漏等

saletw@abpsecurite.com +886-2-2740-7198 台北市中山區南京東路三段 208 號 9 樓