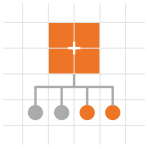
Argos™
鑑識資料視覺化

可視化您的網路架構 深入分析協助決策

Cyberint

現今的資料無所不在。從表面上來看，龐大的資料似乎使調查資安事件獲得最佳結果變得更加簡單和快速。然而事實上，資料的零碎和孤立的性質意味著幾乎不可能將各事件作關聯並擷取有意義的見解。雖然企業組織不遺餘力地收集資料以助其更深入了解事件和指標，但是其中大部份的數據資料實際上卻永遠不會被用到。



鑑識資料視覺化 (Forensic Canvas) 揭開背後的真相

未被深入分析的資料就等同無所用處。

分析師需要合適的工具以助其發現不同資料節點之間的關聯，並針對威脅提供背景訊息。鑑識資料視覺化模組是屬於 Argos™ 平台的一部份，它以自動化、視覺化和直覺性的方式，為分析師提供對入侵指標 (Indicator of Compromise, IOC) 進行分類和研究所需的所有工具和豐富的資料。

藉由運用透過 Cyberint 智能威脅情資 (Threat Intelligence) 功能的數個資訊來源，加上全面覆蓋暗網 (Darknet)、深網 (Deep Web) 和開放網路 (Opennet) 市場，以及駭客論壇、Pastebin 線上平台、聊天室、非公開性的論壇及額外的來源，鑑識資料視覺化能發現並以視覺方式顯示先前未知的關聯、攻擊面向 (Attack Vector) 和相關的威脅參與者，讓分析人員能夠揭開 IOC 背後的真實身份和來源。

分析師利用點選方式就能運用此視覺化模組將 IOC 擴展到其它使用各種來源的已知關聯。此類來源包括：

- **新註冊的網域探索**
- **擴大的 WHOIS (網域查詢機制) 資料庫搜尋**
- **被動式 DNS 資料庫**
- **惡意的檔案雜湊 (File Hash) 資料庫**
- **社交網路的自動探索**

分析師能借助鑑識資料視覺化模組識別出新興的威脅並對其做出回應，使其無法入侵網路，從而主動偵測惡意情資和攻擊。在縮短回應時間及在威脅變成有害的事件之前加以阻止，便是關鍵所在。

有了鑑識資料視覺化模組，分析師便能：

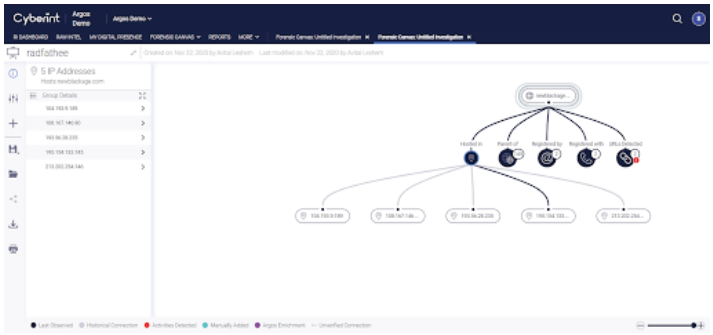
- 在進行調查期間將重心擺在新發現的入侵指標(IOCS)
- 探索所有關聯資產的解釋資料（Metadata），以立即了解與目前調查的相關性
- 以手動方式加入額外資訊，以發現看似無關的實體之間的潛在關聯
- 以可以採取行動和直覺性的方式了解與目前調查的關係
- 建立包括惡意活動時間表在內的威脅參與者特性檔案

鑑識資料視覺化模組的運作方式

鑑識資料視覺化模組的顯示板（Dashboard）能緊密地關聯並顯示豐富的視覺化資訊，而且此資訊可立即用來加強和支援分析師的工作。以下是它運作的方式：

1

以 IOC 著手並自動發現直接的關聯

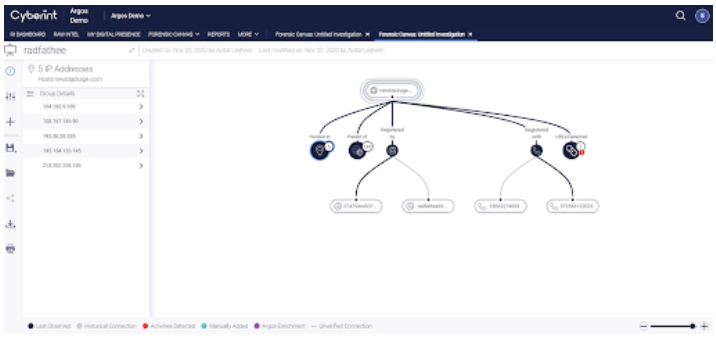


2

擴大調查攻擊基礎架構

3

分析並識別所有威脅參與者



4

查看來自多個資料來源，包括 ARGOS™ 威脅情資增強 (Intelligence Enrichment) 在內的強化情資

鑑識資料視覺化
協助分析師看得更深、發現更多

有了鑑識資料視覺化模組，分析師便能將孤立的資料點轉化為真正的見解，從而做出更好、更快且更理想的決策。如欲了解更多關於鑑識資料視覺化模組的資訊，請與我們聯繫。

> 我們淹沒在大量的資訊當中，同時極需要從中取得精華。
>
> E.O. Wilson

客戶證言

> 「鑑識資料視覺化模組揭露出看似獨立的資料點背後更深層次的內情及關聯。如此豐富的視角為我們的團隊提供所需的見解，讓我們能在危害造成之前做出最理想的決策，並且讓事件緩和下來。」

總結：

- **研究並調查特定的入侵指標（IOC），包括 IP、網域和威脅參與者等等。**
- **取得用於分類和事件回應的強大視覺化功能**
- **根據每個調查的 IOC 使用自動化工具發現關聯和額外的資料**
- **擴大涵蓋新註冊的網域、被動式域名系統（DNS），惡意的檔案雜湊（File Hash）、社交網路帳戶等等。**

使用案例：

- **攻擊基礎架構調查**

  深入了解方法、惡意軟體及其關聯以增進理解

- **威脅參與者分析及識別**

  自動透過威脅情資和社交媒體的探索來蒐集資訊

- **收集威脅細節以作為當前和未來的參考**

  根據技術細節、特徵和行為將特定的攻擊做分類，並將這些攻擊歸類到威脅參與者群組和特定產業以供未來之用

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

Cyberint