以應用程式為中心的網路威脅偵測

近年來，大多數的企業組織已經了解到預防性安全方法已經無法阻止所有攻擊或威脅，因此對於安全團隊而言，預防這些入侵和漏洞變得更現實及關鍵以避免數據及財務的損失。相同的，大多數的攻擊不再以「粉碎及侵占」模式進行，而是繞過安全系統邊界後進入內部網路以「隱形」模式進行內部偵查。這為攻擊者提供了千載難逢的好機會來深入研究整個部署架構，還能夠掃描更多內部資產來進行後續的控制以及破壞。儘管所有組織都具有周邊安全系統，有時在重要伺服器和桌機也安裝有帶代理程式的端點防護，然而一旦威脅進入內部並橫向移動，它們就無法達成保護內部主要任務。

Uila通過提供即時和全面的服務來幫助企業組織應對高級網路威脅，以應用程式為中心的洞悉力協助混合企業對於橫向移動的威脅。

無代理程式的網路威脅監控

無代理程式及可擴展部署模型能夠針對關鍵應用程式識別威脅挑戰，並針對3200多個應用程式進行分類。

應用程式的異常排除

實時追蹤主要應用程式工作負載特徵，以識別異常行為，例如關鍵應用程式和基礎架構資源之間的連結關係更改，新的虛擬器的刪減或增加等等。

以應用程式為中心的橫向移動威脅監測

全面可視化以應用程式為中心的橫向（東西向）移動流量並自動警告網路威脅，例如惡意軟體、DDos(分散式阻斷服務攻擊)、C&C、端口掃描以及攻擊套件等。

提供對於威脅的結論性關鍵證據鏈

識別攻擊之前、期間和之後的所有應用程式數據、基礎架構狀態和網路流量數據。

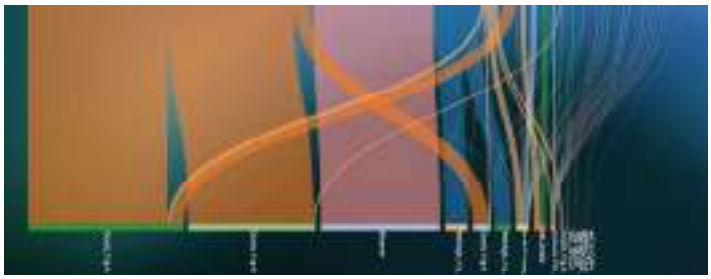
實時偵測對於數據中心及雲端工作負載的高級惡意威脅

- 實時偵測數千種新興威脅，包括勒索軟體、命令與控制(C&C)、攻擊套件、惡意軟體攻擊、端口掃描、程式碼混淆、SMB 攻擊，以及緩衝區溢位攻擊等等。
- 偵測引擎使用自致力於網路安全行業發展的最大集團之最新的認證支援與更新。
- 全面了解威脅的方式、來源、對象，及時間等歷史背景。
- 詳細了解從數據中心到網路的出口流量，並減少與常規網路連接相關的部分風險。

應用程式異常偵測

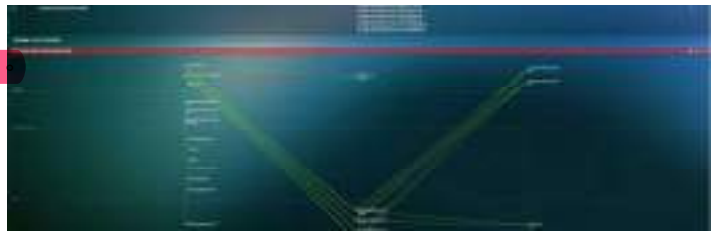
- 自動對3200多個應用程式進行分類並呈現應用程式與基礎架構之間的依存關係。
- 識別未經授權的虛擬器及其橫向移動。
- 利用拓撲圖可視化多層應用程式資產之間的依賴關係的新增或減少，達到辨識網路攻擊的目的。
- 將數千種網路威脅直接映射到應用程式性能與其關聯的異常行為，以識別根本原因。

橫向移動流量分析



- 全面可視化橫向移動流量模式以識別自定義後門及受損之系統。例如可能用於傳輸文件、惡意軟體、密碼轉除程序的SMB、SMB2協議。
- 辨識未經授權之虛擬器、伺服器、連結以及現有部署的流量模式更改。

深入洞悉當前資產和潛在受威脅之資產

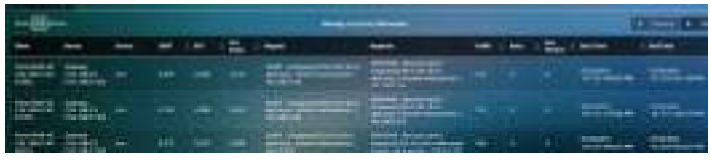


- 獲取有關受損系統的關聯性，進程和基礎架構的詳細訊息（CPU核心數，CPU容量，記憶體，網路流量）
- 了解您當前受到威脅的系統如何作為多層應用程式的一部分連接到其他關鍵的虛擬和物理資產，以深入了解下一步可能受到威脅的資產。

識別數據洩露活動

- 詳細了解從數據中心到網路的流量洩露，並減少與常規網路連接相關的大部分風險。保持對那些未經控制並可能在非同意的情況下將專有訊息移至異地之電子郵件或文件傳輸的完全控制，並防止您的網路成為DDoS攻擊的對象。有時在這些對外交易行為中可能顯示數據的洩露。
- 識別和分類那些已由Spamhaus(www.spamhaus.org)識別將數據洩露到垃圾郵件網路的訊息及和DShield列出的頂級攻擊者(www.dshield.org)。
- 可視化對外流量詳細訊息，包括虛擬器內部詳細訊息、目標IP、目標伺服器位置，及對外流量的應用程式與服務等。
  在世界地圖上可視化出站路徑目的地。
  僅針對關鍵服務、應用程式組自定義和篩選對外流量詳細訊息可視化。

提供對於威脅的結論性關鍵證據鏈



- 保存詳細的數據，以協助安全維護人員確定網路威脅何時以及如何開始。
- 在應用程式層進行詳細的交易分析，以分析混合環境網路遭受攻擊開始時之資訊。
- 補捉封包以獲取鑑識性證據或進行進一步分析。