IMPERVA

Imperva Attack Analytics
雲端AI告警分析系統

DATASHEET

資安團隊現今所需面臨的挑戰包括：

- 資安系統每天都會發送數以萬計的告警。
- 單靠人力難以分析所有的告警事件。
- 無法在眾多告警事件中，即時辨別真正的威脅。
- 缺乏對所有應用程式攻擊提供單一、具整合性的分析介面

在眾多告警事件裡找出真正的威脅

由於持續發生資料外洩、複雜的威脅與超量的告警事件，資安分析變得越來越繁瑣、複雜。隨著企業逐步將應用程式移轉到雲端，無論是在內部、雲端、或是混合式環境，保護應用程式都變得越來越複雜。

IT 團隊需要適當的資訊與分析能力才能明確回應並解決資安事件。針對系統提供的大量資料，使用AI人工智慧及機器學習，是辨別即刻威脅的唯一方式。

Imperva Attack Analytics 雲端AI告警分析系統將成千上萬的告警事件相互串聯，並縮減至幾個簡要的說明。Attack Analytics 採用AI人工智慧及機器學習，讓應用程式的資安事件分析變得簡單，同時也讓 IT 團隊能針對真正的資安威脅採取快速且正確的因應措施。系統會將告警事件依屬性及嚴重程度分門別類，以便透過機器學習技術進行快速調查。強大的深入分析功能讓資安團隊能針對鎖定的攻擊事件進行重點分析。

Attack Analytics 是 Imperva 應用程式防護解決方案之一，整合 SecureSphere 及 Incapsula 網路應用程式防火牆(WAF)所提供的告警事件訊息，並提供資安事件所需的統一監控及統整分析。

圖1：Attack Analytics 將成千上萬的告警事件縮減至幾個簡要的說明。

將資安告警去蕪存菁

提升營運效率

Attack Analytics 將大量 WAF 告警縮減至幾個簡要說明，藉此降低資安事件分析所需的時間。在事件處理量大幅降低的情況下，資安團隊的營運效益也因而獲得顯著提升。

降低風險

Attack Analytics 將告警事件分類並排定優先順序，進而降低資安事件調查分析的複雜性。這讓資安團隊可以用簡單的方式，專注在少數幾個真正重要的事件分析上，而不必在成千上萬的事件告警裡大海撈針。AI 人工智慧的導入，能降低隱藏在大量告警事件下的威脅風險。

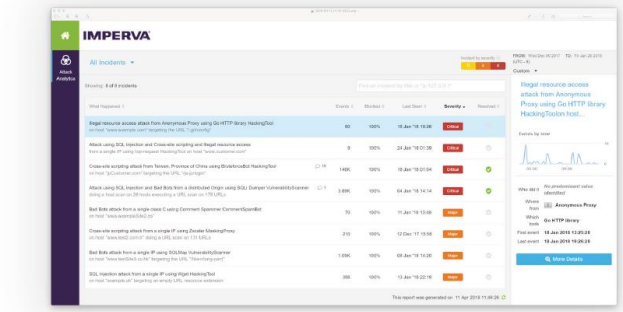

圖 2 ：單一、具整合性的 WAF 告警分析介面

單一控管介面

當企業開始部署雲端資安項目以保護雲端應用程式及API，監控企業整體的資安事件也變得更加困難。Attack Analytics 提供單一介面，控管所有 Imperva 雲端及內部網路應用程式防火牆所產生的告警事件，進而提供完整可視性，協助企業控管內外部資安攻擊。

全球性的洞察分析

Attack Analytics 運用AI人工智慧，彙集在全球所蒐集到的事件資料，並加以分析、辨別各種攻擊型態。這些資訊在判斷駭客是採取常見攻擊或新的手法上，具有相當大的價值。Attack Analytics 所提供的彙整性智能分析將能幫助企業快速辨別各種攻擊。

適用雲端環境

Attack Analytics 是雲端防護解決方案，因此可一鍵部署，沒有規模限制，並能依企業需求設定告警事件的接收處理數量。

圖3：可擴充的雲端防護解決方案

Imperva 應用程式防護解決方案

Imperva 應用程式防護解決方案採用靈活的混合模式，將雲端服務結合虛擬、實體設備，進而提供應用程式防護和DDoS防禦。Imperva SecureSphere 提供可在企業內部或雲端部署的實體及虛擬設備；而 Incapsula 則提供各種雲端防護服務。

Attack Analytics 從 SecureSphere 和 Incapsula Web 應用程式防火牆收集告警事件資料。系統從實體、虛擬和雲端部署設備中收集資料，並透過AI人工智慧加以分析，提供企業在應用程式防護上的綜觀洞察。Attack Analytics 雲端AI告警分析系統支援 Incapsula 雲端防護和 SecureSphere 網路應用程式防火牆系列產品。