MANDIANT

MANDIANT ADVANTAGE
資料工作表

Security Validation

證明網路安全的價值

CISO 必須證明資安防禦能力的有效性

如今，具有風險意識的商業環境為 CISO 及其團隊帶來前所未有的壓力，要求他們保護公司資產，並保護其組織的財務狀況與品牌價值。他們必須向領導階層證明其網路安全投資的價值，及其在防止對手入侵關鍵系統方面的有效性。

但是缺乏驗證資安防禦能力有效性、量化風險及展示營運能力所需的工具，他們只能依靠漏洞掃描器、滲透測試、紅隊演練或入侵與攻擊模擬來證明自己。由於固有的局限性，這些方法不足以評估防禦能力有效性，也不能對組織面臨的具體、高優先順序威脅提供相關和及時的見解。

Mandiant Advantage Security Validation 持續地接收 Mandiant 有關最新攻擊者 TTP 的前線資訊情報，並自動執行測試程式以提供有關您安全控制執行情況的實際資料。這個解決方案提供您安全控制有效性狀態的可見性和證據，以應對針對您組織和資料的對手威脅，來最佳化您的環境以免受相關威脅。

證明安全有效性並量化您的風險

處理得當的資安防禦能力驗證是以五步方法為基礎，該方法可洞悉要測試的最重要內容，以及如何根據可能會針對組織或產業的人員和物件的知識來優化防禦。

圖 1. Mandiant 五步情報主導防禦能力驗證方法。

這種方法需要能即時利用威脅資料。Security Validation 使用 Mandiant 威脅情報與事件回應資料揭示攻擊者現在正在做什麼。借助情報主導的 Security Validation，安全團隊可以識別針對您組織的高優先順序威脅，並根據可能會對組織構成威脅的人員或物件的知識來建立驗證策略。憑藉 Mandiant，資安領導及其團隊可以在技術、流程與人員上執行完整、持續的資安控制驗證。

Mandiant Advantage 結合創新的驗證技術、業界領先的威脅情報和 Mandiant 所具備的專業知識，協助安全團隊針對安全控制執行真實的攻擊行為。這讓他們能夠快速量化並證明其資安計畫的有效性，以及防禦最複雜對手攻擊的能力。

Security Validation 讓團隊能夠：

- 驗證您面對重大威脅的安全有效性
- 根據無可比擬的 Mandiant 威脅情報與事故回應資料，安全地執行相關攻擊
- 發現組織的資安基礎設施中未偵測到的缺陷
- 確定最大的優化機會
- 隨著時間衡量對防禦措施的改進
- 捕捉所需的證據來證明您投資於資安的效率和價值

圖 2. Security Validation 幫助實現視覺化並產生證據，表明您的控制正在保護關鍵資產。

Security Validation 具備進階功能：

- **威脅發動者保障**可針對活躍威脅發動者及其 TTP 進行安全控制測試。這個進階的能力與 Mandiant Threat Intelligence 和產業領先的威脅情報合作夥伴第三方整合，使您的安全程式能夠實現最佳保護。
- **進階環境偏離分析**支援對 IT 基礎設施的持續監控，以消除環境偏離，並推動對防禦回歸的持續驗證，從而確保組織資安基礎設施的健康。
- **Protected Theater** 安全地執行惡意軟體、勒索軟體及其他破壞性攻擊，以驗證端點控制的效能，實現對最新與新興威脅的主動保護。

Security Validation 產品系列包括多種部署選項：

- **驗證即服務**。依照顧客期待的業務成果或特定威脅，Mandiant Advantage 提供持續且自動化的驗證和報告解決方案，利用 Mandiant 驗證技術、Mandiant 專家諮詢和業界領先的威脅情報。
- **所有威脅驗證**。雲端型（資安即服務 (SaaS)）或部署為現場虛擬裝置。
- **受管或共同受管驗證**。根據客戶的預期業務成果，Mandiant 團隊建立了持續驗證和報告計畫，以適應特定使用案例，持續向客戶利益相關者提供詳細報告。

Security Validation 的業務效益

衡量有效性和證明投資價值

獲取可量化的資料，幫助確定提高資安有效性所需的投資，並量化您的總體風險狀況。資安團隊也可以使用此證據來向行政領導和董事會證明安全投資價值的合理性。

併購與收購

清楚地掌握正在進行併購或收購的公司在控制方面如何存在重疊或缺陷。透過開支合理化，您可以計算合併的潛在美元數額，以及因併購而可能承擔的風險等級。

僱用和培訓資安人才

看看過去幾年的經驗並評估資安專業人士的學習潛力、他們所擁有的經驗類型，以及在現實世界情境中 他們的技能組合與您所在組織的環境匹配程度。透過在其生產環境中安全地執行真實攻擊，IT 領導者可以監控潛在申請者會如何回應並作出反應 IT 領導也可以開展定期評估 作為培訓練習，瞭解團隊在現實世界攻擊情境中，是否展現出可接受的回應時間和所需的技能。

品牌保護

主動並持續測量資安防禦能力的有效性，以減少遭受入侵或攻擊的風險，並保護您的品牌聲譽和客戶忠誠度。

資料隱私與保護

保護客戶資料並確保遵守監管、公司和第三方要求。

由 Mandiant Advantage Threat Intelligence 提供的 Security Validation

在過去超過 15 年的時間裡，透過全球各地的調查、事件諮詢及紅隊演練，Mandiant 已經建立並策劃了一個獨特的威脅情報產品，並持續以新的證據資料、人類專業知識及獨特的分析間諜情報計數來不斷更新產品。透過以下平衡的來源組合，Mandiant 現在主導著網路威脅情報領域：

- **入侵情報**，透過 Mandiant Consulting 事件回應業務收集入侵情報
- **對手情報**，Mandiant 研究員獲取對手情報
- **機器情報**，來自業界領先的第三方偵測器和控制
- **營運情報**，源自 Mandiant Managed Defense 服務的營運情報

請在 www.mandiant.com 上瞭解更多

Mandiant
11951 Freedom Dr, 6th Fl, Reston, VA 20190
(703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com

關於 Mandiant

自 2004 年起，Mandiant® 就一直是具有資安意識之組織值得信賴的合作夥伴。如今，產業領先的 Mandiant 威脅情報與專業知識所推動的動態解決方案能幫助組織制定更有效的計畫，並增強其對網路準備度的信心。

MANDIANT®
YOUR CYBERSECURITY ADVANTAGE

M-EXT-DS-ZH-TW-000317-05