IBM Security

化雜訊為力量
用資安大數據建構堅實防禦！

面對排山倒海而來的資安數據，IT人只能選擇默默地被數據淹沒、
直到災難發生的那一刻？這樣的資安日常，不能再繼續下去！

企業每天面對超過
20萬次
資安事件，您能一一辨識嗎？

攻擊不息，雜訊不止
QRadar為您力挽狂瀾

資安分析師每天面對千百種資安弱點、威脅與攻擊。每分每秒，資安防護措施傳來海量的事件與數據，若無法解讀其意義，就只能視為雜訊而忽視，逐漸累積成災。QRadar能在茫茫數據中為您過濾雜訊，即時聚焦於關鍵事件與警訊，幫助您快速採取必要行動，精準打擊威脅！

使用者　雲端　網路　資產

解讀安全數據
將Log記錄檔與網路流量數據標準化與一致化，以供更精準深入的分析。

異常行為監測
歸納資產、使用者、服務與網路活動的行為基準，建立常態模型，用以精準監測異常行為。

進階分析

行為模式分析
即時分析資安事件特徵，比對已知惡意威脅模式，快速辨識與分類資安威脅。

異常行為偵測
以「正常行為模式」持續檢測與辨識，找出可能帶來威脅的異常行為。

歷史資料分析
當攻擊者採取異常步驟來侵入系統，系統可即時偵測到這些非預期行為並立即預警。

統計分析
透過統計數據察覺潛伏的威脅，例如有終端設備異常送出大量資料給未授權的雲服務等。

設備行為偵測
持續監控實體設備，掌握非常規行為，服務與連線，當系統被入侵時可更快察覺並介入。

使用者行為分析
持續分析個別使用者行為，偵測偏差行為，及時找出被入侵的使用者或有惡意的內賊。

使用者分群監測
依據相同的使用行為將使用者分群，持續監測每個分群中的異常行為，可更快速、更精準地辨識風險與找到惡意使用者。

掌握最新資安情報
交叉比對事件特徵與資安威脅情報，例如惡意網域與雜湊值(Hashes)。當遭受到最新型態攻擊時可快速察覺與應變。

預測分析
運用行為預測模型，提前預測並偵測未來可能發生的異常行為。

預警！
整合分析結果、串聯相關信息，建立從端到端的資安事件關聯鏈，判斷其嚴重性，並即時、自動發布警報。

事件調查

根因　攻擊者

AI賦能・智慧推理
運用自然語言處理技術自動建立知識圖表，推理事件根因，提供攻擊的概觀，並且分辨相關的入侵指標

面對大量威脅，您可以高枕無憂！
有感提升防護速度、偵測數量與精準度，防禦網路攻擊

QRadar協助資安分析師在成千上萬的日常事件中精準掌握重點，聚焦於可疑事件，避免大量資料造成的混淆與延誤，並提供清晰明確的應對方案。
在AI人工智慧分析技術與全球最新、最完整的資安情報輔助下，大量資安數據不再是無意義的雜訊。每一筆資訊都能幫助您提升整體安全性，成為守護安全的重要資產！

前往 www.ibm.com/tw-zh/security/security-intelligence/QRadar 開始免費試用

IBM Security

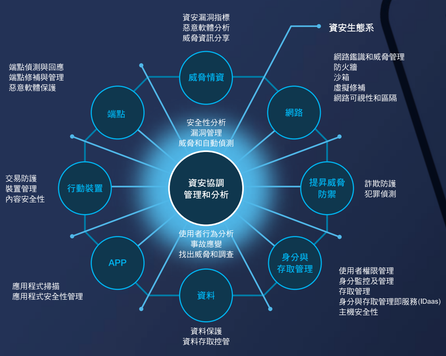
與威脅共存—打造「安全免疫系統」

認清現實吧！

資安攻擊不斷進化，沒有任何企業與組織能夠完美擋下所有攻擊，然而您可以在受到攻擊後，守住關鍵資料、流程與客戶體驗，毫髮無傷全身而退。這就是最新一代資訊安全：「安全免疫系統」。

「安全免疫系統」以 IBM QRadar 作為核心，整合來自終端設備、雲端、網路、使用者、外部威脅情資的資訊，即時呈現全面深入且精準清晰的資安整體視圖。IBM QRadar 協助 IT 管理者快速偵測威脅，依據風險等級規劃事件優先順序，並根據智慧分析結果採取必要行動，有效隔離風險、防止傷害。

正如人類免疫系統能讓我們與病毒共存，遭受入侵時快速辨識外來威脅，並施以必要的阻絕及消滅。「安全免疫系統」將取代傳統「全面阻絕」的防禦策略，成為未來企業管理資安的主流做法！



為何您需要「安全免疫系統」？

從百萬可能中找到真正威脅

根據天文統計，每天至少有數十億顆隕石進入大氣層，但曾造成生態滅絕的只有 6500 萬年前的那一顆。同樣的，當每天有數十萬筆資安事件排山倒海而來，您能找到真正威脅嗎？還是只能視而不見、直到災難來臨？

化雜訊為資安防護力量

企業建置的資訊安全防護設備與措施，每分每秒都在產出大量資訊。若能及時解讀資訊的意義，就能採取必要行動，預防資安災難發生。反之，若沒有能力解讀，這些資訊就只是毫無用處的大量雜訊。

以人工智慧對抗人工智慧

惡意攻擊不斷進化，已經能運用人工智慧技術模仿自然行為，進行大規模、自動化、快速、精準且深入的攻擊行動。要與之抗衡，企業也必須擁有同等級 AI 能力，協助管理者過濾與篩選關鍵資訊，及時採取應對措施。

讓時間站在您這邊

攻擊者永遠是主動的一方，這不代表您只能坐以待斃。流行性病毒有潛伏期，資安攻擊亦然。網路罪犯平均都潛伏期達 191 天。而資安事件發生後，也需要數天至數月的時間來清查原因、鑑識問題。事實上，所有的威脅都有跡可循，QRadar 近乎即時的洞悉能力，在火苗燃起之前及早撲滅，並在攻擊發生後及時找出原因、修補。

輕鬆管理法規遵循

2018 年歐盟 GDPR 通用資料保護規則實施，監管規則更加嚴格，若有違反最高將面臨 7.2 億台幣（2 千萬歐元）的巨額罰款。於此同時，世界各國也在調整法規，要求企業更加嚴謹的管理個人資料與關鍵營運資訊。

資安是一場無止境的戰爭

科技不斷進化，惡意攻擊持續升級，加上人工智慧的輔助，資安攻防將永遠沒有歇止的一刻。但若要實施嚴密控管，資安成本可能飆高，企業的數位創新也可能會受限。

資安管理是動態的進行式，必須在成本與風險之間不斷調整，求取最佳平衡。要避免陷入資安「軍備競賽」的困局，就必須掌握全局、精準決策。身為企業資安守門人，您的首要之務是建構資安環境的完整脈絡與詳盡數據分析，才能言有所本、行有所據。以 IBM QRadar 智慧安全分析平台為核心的「安全免疫系統」，正是為此而生。

IBM QRadar 智慧安全分析平台
連續九年榮獲 Gartner SIEM 魔力象限領導者殊榮

被資安數據淹沒的痛苦，我們懂

孫子兵法云：「知己知彼，百戰百勝。」在資安戰爭中，這句話更是顛撲不破的真理。

知己，是掌握 IT 系統中每天發生的各種事件、紀錄、統計資料與使用者行為。

知彼，是了解全球最新駭客攻擊手法與模式，才能與內部發生的跡證交叉比對，防範未然。

然而，在企業資安領域，知己知彼絕非易事。IT 環境日趨複雜，企業部署多種防禦措施，各自獨立運作互不溝通，每天產出數十萬筆 log 與告警，資料量之大讓 IT 團隊無法解讀、難以利用！

企業規模不論大小，面對的資安風險都是同樣嚴峻。IBM QRadar 的任務，就是幫助各種規模的企業及時感知威脅、偵測潛在風險、解讀龐大數據、做出正確因應。

IBM QRADAR 重要功能

- 感知並偵測詐騙、內鬼和進階威脅
- 立即將事件正規化並產生相互關聯
- 感知、追蹤並連結重大事件和威脅
- 在內部部署或雲端環境中部署 QRadar SIEM
- 快速實惠地新增更多儲存空間和處理能力
- 強制執行資料隱私原則
- 從 IBM X-Force 提供威脅情報專業
- 實現威脅預防協同作業和管理
- 整合數百個 IBM 與非 IBM 產品

我家也有福爾摩斯。
IBM QRadar Incident Forensics
資安事件鑑定只要短短幾分鐘！

系統遭到攻擊，當務之急就是還原過程、鑑定原因、修補問題。鑑識所需時間越長，暴露風險就越大。多數企業需要費時數天才能完成鑑識，早已無法因應瞬息萬變的資安賽局！

IBM® QRadar® Incident Forensics 可幫助您追蹤潛在攻擊者的逐步動作，快速進行惡意資安事件的深度鑒定調查，鑑識時間由數天縮短為數分鐘，並協助您重新修補安全漏洞，避免再次遭受攻擊。

豬隊友狀況外？內賊難防？
交給 IBM QRadar UBA ！

相信每一位資安專家都會同意：「人，是資安防禦最不可控的環節。」IBM QRadar 使用者行為分析 (UBA) 能夠即時分析內部人員的使用行為與活動模式，及早發現可疑的異常行為，並判斷其風險。

QRadar 具備智慧分析能力，協助資安管理者將龐大使用者資料去蕪存菁，發掘異常行為、橫向移動、惡意威脅與資料竊取等潛在風險，及時預警與資安儀表板。管理者可快速鎖定使用者進行調查，提早因應防範未然。

看不完的日誌裡，藏著 IT 最深的恐懼。
讓 IBM QRadar Network Insights 為您分憂解勞！

每天收到爆滿的資安日誌 (log)，明知這惡意風險的蹤跡就藏在其中，卻無法解讀！ IBM QRadar Network Insights 正如其名：這是個網路威脅的偵測雷達，能夠即時分析網路流量與日誌數據，將隱藏的威脅嚇在陽光下！

IBM QRadar Network Insights 可快速執行深度鑑定，將資安事件調查時間從數天縮短為數分鐘，大幅減少團隊調查威脅所需的的時間與心力，並協助修補網路安全漏洞，預防災難再次發生。

Who 怕 Who ？用 AI 戰勝 AI ！
IBM QRadar Advisor with Watson 給您滿滿的 AI 戰力

人工智慧 (AI) 被網路犯罪份子用於攻擊行動的案例，在國際上已時有所聞。AI 不僅讓網路攻擊加速、自動化，更可模仿自然行為，達到更廣泛的社交工程與網路釣魚目的。

聽起來很可怕？好消息是，您也能用 AI 來戰勝 AI ！ IBM IBM QRadar Advisor with Watson 是 AI 界的資安專家，遍讀全球無數資安報告、新聞、研究，並建立完整「知識圖譜」(Knowledge Graph)，能快速分析非結構化資料，並建立安全攻擊的關聯性，輔助資安人員全天候 7x24 預測攻擊、即時回應！

有漏洞並不可恥，堵起來就是了。
IBM QRadar Vulnerability Manager
幫您秒補資安漏洞！

IT 環境越複雜，來自軟硬體的漏洞及其暴露的資安弱點就越令人防不勝防。IBM QRadar Vulnerability Manager 可以掃描完整網路環境，自動偵測超過 7 萬個已知風險，並結合外部資訊隨時更新，制定優先因應方案，搶在攻擊發生前就阻絕外患。

打群架更有勝算！
IBM Security App Exchange 與全球頂尖夥伴共禦外侮

資安攻擊是全球企業共同面對的挑戰，IBM Security App Exchange 結合產業頂尖合作夥伴、開發者與資安工具，您從此無須單打獨鬥！透過這個協作平台，您可將各種立即可用的解決方案整合到 IBM Security，快速建立您所需的防禦工具，並與產業共享最佳資安實戰作法。