
CYBERSEC 2022 臺灣資安大會
CHANGE NOW
數位轉型 資安升級
SEP. 20-22 臺北南港展覽二館

正面迎擊威脅挑戰

數 位 轉 型　資 安 升 級

Ted Liu
IBM Security

liuted@tw.ibm.com

IBM Security

SEP. 20-22 臺 北 南 港 展 覽 二 館

自動偵測、即時回應的智能資安解決方案

SEP. 20-22 臺北南港展覽二館

IBM 全球資訊安全市場定位與商業策略

企業等級資安方案

- 15個資訊安全解決方案領導者
- 130個國家地區、8,500名資訊安全專家，千餘位十多年經驗的駭客專家、事件回應團隊與威脅情資分析師
- 23年來陸續併購23個資安產品，持續豐富整體解決方案

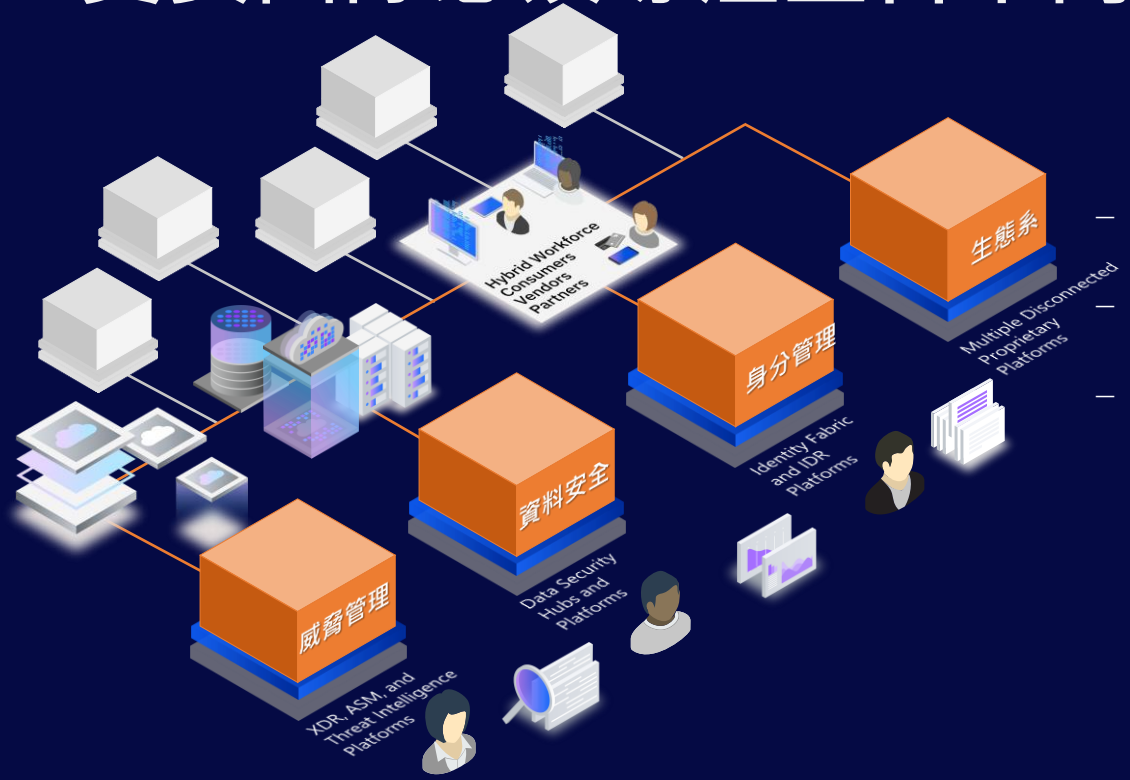
AI 資安防護的先行者

- 威脅偵測與回應管理
- 資料安全保護與稽核
- 身分認證與存取管理
- 防範與偵測金融詐欺
- 資安策略、風險與合規
- 雲端安全服務

專業可信賴的資安服務

- 資訊安全顧問與諮詢
- 資訊安全代管服務商
- 先進科技工具提供商

資安團隊必須專注整合不同工具與資料



- 66% 的資安團隊無法共享資料
- 資安工程師必須手動整合各種工具
- 整合耗時且昂貴

需要統一、開放和零信任的方法

跨不同領域上下文、見解與編排

建立零信任策略

- 建立最小特權
- 持續驗證
- 假設入侵

採用統一開放的方法

- 開放式架構連結工具、資產與情資
- 共享上下文、分析與風險見解，做出更好的決策
- 自動化工作流程，快速回應資安威脅

QRadar XDR 開放資安平台實現零信任策略

使用開放標準連接各種資安工具，取得跨領域間各種資安見解

連結	連接各種工具間的重要資安資訊，實現全方位洞察
豐富	威脅情資提供跨平台與跨領域資訊
分析	提供彈性且功能強大的分析功能
了解	透過風險管理了解威脅與漏洞的危害性
協作	案例管理幫助安全團隊協作、分析與簡化工作流程
體驗	提供統一使用體驗、降低學習成本

通過開放的安全平台獲得洞察力並節省時間

使用開放標準和最佳實踐整合**人員**、**流程**和**工具**

連結安全資料

連接各工具與資料湖泊，打破資安工具孤島

工作流程

使用通用 UX、集中自動化、案例管理與劇本，能更快速的採取行動

共享資安訊息

利用共享的資料、資產與威脅情資做出更好的決策

雲原生架構

現代化的安全架構，可在任何地方執行

IBM Cloud Pak for Security

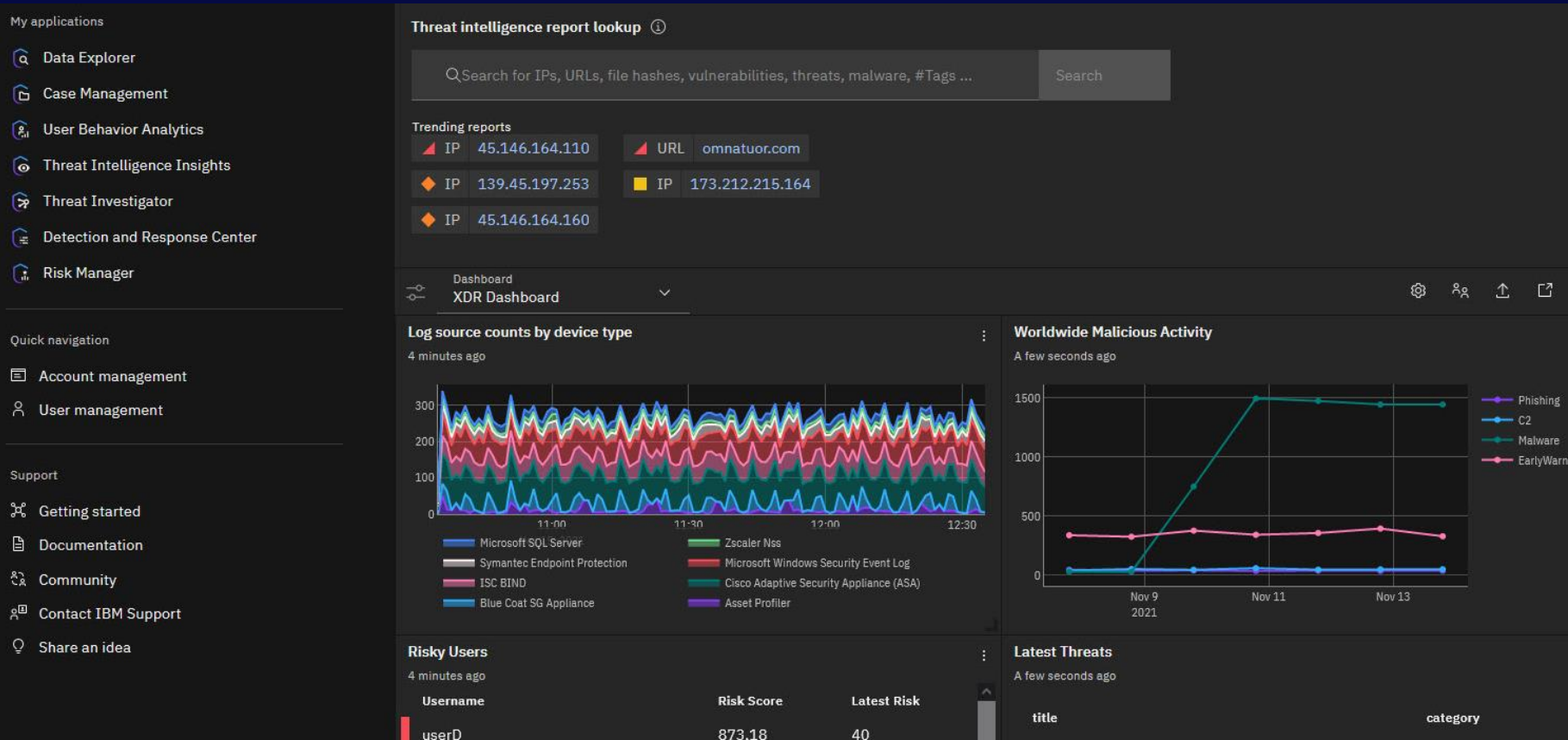
Cross-domain security context, insights, and orchestration

- Threat Management
- Data Protection
- Identity and Access

Common UX
Shared Analytics
Unified Playbooks
Global Threat Intelligence

Red Hat OpenShift

開放資安平台實現零信任策略



簡化威脅管理

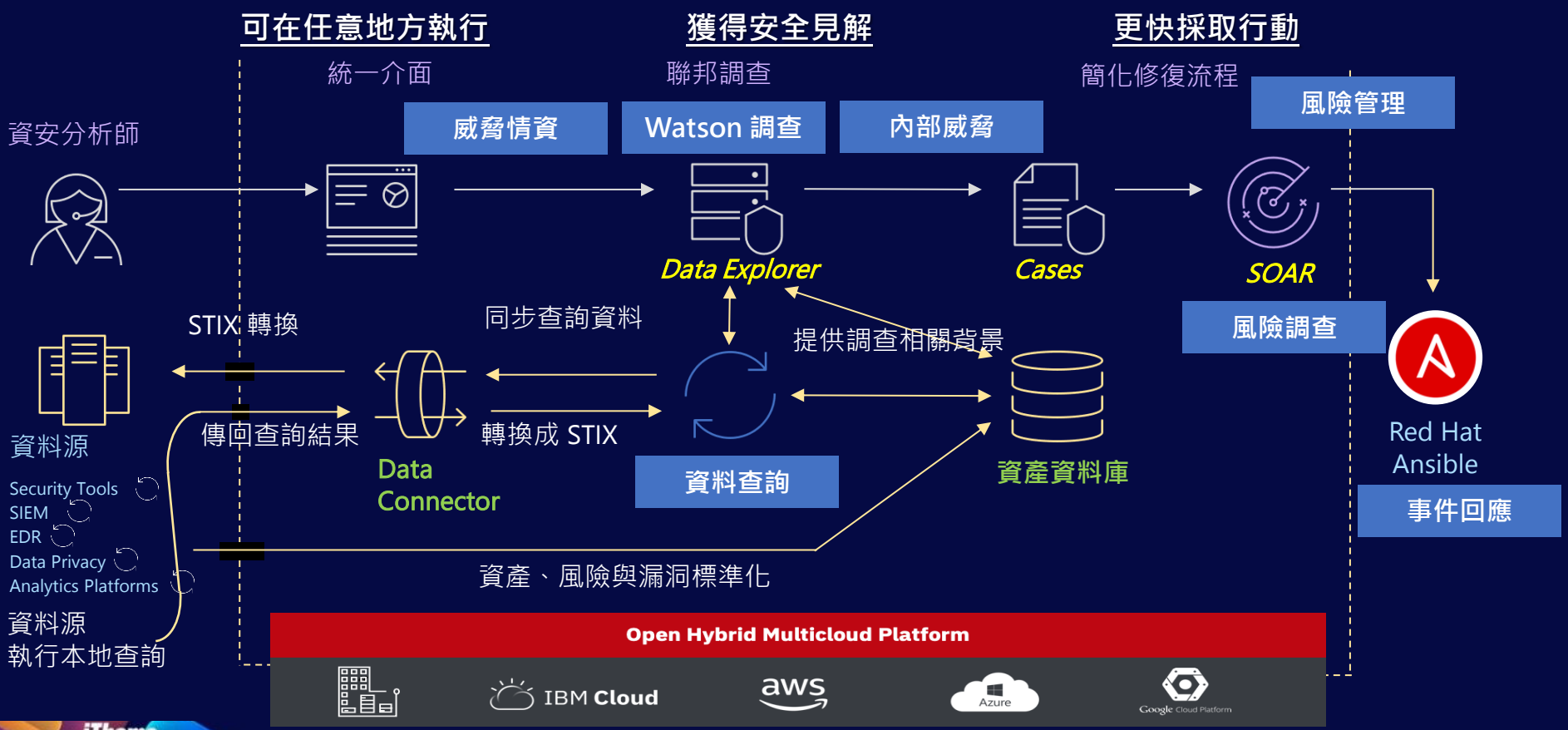
QRadar XDR

QRadar XDR Connect

IBM XDR 連接各種資安工具實踐 SOC 自動化

Open Source and Standards

QRadar XDR 執行流程



正面迎擊威脅挑戰

進階分析
準確偵測使用者、網路、系統和應用程式的各種威脅

提高生產力
透過工具更容易獲取資料與管理系統

簡化工作流程
幫助分析師做出更快、更明智的判斷

利用 QRadar XDR 更精確的偵測與管理威脅
降低資料洩露和業務中斷的風險

pdc 北祥資訊
Pershing Data Corporation

Distributor IBM