IBM Resilient Security Orchestration, Automation and Response on Cloud

本「服務說明」說明本「雲端服務」之內容。適用之訂購文件提供 貴客戶訂單有關計價及其他詳細資料。

1. 雲端服務

IBM Resilient Security Orchestration, Automation, and Response (SOAR) Platform on Cloud 可供組織對事故因應相關人員、程序及技術進行編配及自動化作業。

IBM Resilient SOAR Platform on Cloud 簡化事故因應與隱私因應管理，進而為組織提供自動化、更快速且更有彈性之事件與事故因應方式。Resilient SOAR Platform on Cloud 為成功建立網路安全防禦奠定基礎，俾使組織得以執行以下列事項：

- 擬訂依業界標準及實作典範所訂定之因應計劃。
- 更易於與安全及 IT 工具整合，以及編配事件及事故因應措施。
- 進行整體組織之協同作業，為各利害關係人提供工具，使其得以依其角色執行各項作業，為事故之因應盡其心力。

IBM Resilient SOAR Platform 係為具有各種規模及複雜性之組織而設計，並可搭配數種選用附加程式一併購買。除 貴客戶所購買之供應項目或附加程式另有規定者外， 貴客戶不得使用各項功能。

1.1 供應項目

貴客戶得從下列可用供應項目選取其所要供應項目：

1.1.1 IBM Resilient SOAR Platform on Cloud

IBM Resilient SOAR Platform on Cloud Orchestration 可為網路安全防禦奠定基礎。貴客戶可依據業界標準與實作典範擬訂因應計劃、易於與安全及 IT 工具整合，以及精心安排事件及事故因應措施。本「雲端服務」可協助進行整體組織之協同作業，讓各利害關係人得以依其角色執行各項作業，為事故之因應盡其心力。

安全團隊可使用平台之依用途而建置之案例管理功能，進行網路安全事件與事故之協同作業。藉由劇本、資料欄位及顯示畫面佈置之客製化，Dynamic Playbooks 可因應快速演變之攻擊，團隊可快速對程序進行反覆運算，進而提高效率。模擬可進一步協助改善因應程序。內建及可安裝整合可提供資料強化功能，以蒐集安全團隊作成決策所需之環境定義，並可依據所購買之「每月動作」數量，進行補救動作之編配作業。電子郵件之汲取與剖析可提供從其他工具提報之輕量型方法。透過 SAML 鑑別可保障存取之安全。分析及產生報告有助於進行透通性與風險分析。下列其他所有附加程式均須要本供應項目。

1.2 選用服務

1.2.1 IBM Resilient SOAR Platform Actions on Cloud

IBM Resilient SOAR Platform on Cloud Actions 可執行平台之編配作業功能。內建及可安裝整合，包括與各種威脅情報資訊來源整合，可提供自動化強化功能，以蒐集安全團隊作成決策及進行補救動作編配作業所需之環境定義。

1.2.2 IBM Resilient SOAR Platform on Cloud Privacy Add-On

IBM Resilient SOAR Platform on Cloud Privacy 可供 貴客戶評量及因應隱私資料外洩。本供應項目所產生之因應計劃可依據資料類型、記錄數量及適用管轄權責進行調整。貴客戶亦可存取內建之全球資料隱私權侵權通知規章知識庫，有助於進一步客製事故因應計劃。

1.2.3 IBM Resilient SOAR Platform on Cloud Team Management Add-On

IBM Resilient SOAR Platform on Cloud Teams 提供跨越多團隊之使用者管理及資料隔離。機密性資訊之保存，以有知悉之必要為依據，利用「工作區」及可客製化角色型存取控制之方式限制存取。利用 Active Directory 進行使用者授權，可簡化使用者與群組管理。另外，亦可將不同群組配置為擁有各自之「組織」。

1.2.4 IBM Resilient SOAR Platform on Cloud MSSP Add-On

IBM Resilient SOAR Platform on Cloud MSSP 提供跨越多「組織」之案例管理、程序、客製作業及劇本管理等功能。來自多「組織」之事件與事故，可從單一佇列予以檢視，為受管安全服務提供者 (MSSP) 分析師提供其客戶之綜合性觀點。內含各「組織」配置之劇本，可提供標準化及客製化程序之簡單管理方式。

1.2.5 IBM Resilient SOAR Platform on Cloud Non-Production Add-On

IBM Resilient SOAR Platform on Cloud Non-Production 係為 IBM Resilient SOAR Platform 之個別實例，貴客戶僅限將該實例使用於內部非正式作業活動，包括且不限於測試、效能調整、錯誤診斷、內部評比、暫置品質確保活動及/或使用已發佈的應用程式設計介面，開發內部使用之「雲端服務」新增或延伸項目。

1.3 Acceleration Services

IBM Security Expert Labs (SEL) for Resilient Services 供應項目為遠端交付服務，可安排 Resilient 專家時間，由專家提供 Resilient 部署有關架構與實作指引。IBM Resilient Security, Orchestration and Response 供應項目 – 作為「雲端服務」或就地部署軟體 – 為前述「服務」之必備項目。

1.3.1 IBM SEL for Resilient Base Starter Service

在 5 日遠端約定中，IBM 將提供下列項目：

- 協助訂定 IBM Security Resilient 架構
- 已安裝及已配置之 IBM Security Resilient（在適用情形下）
- 對「分析師」與「設計師」進行 貴客戶現行「事故因應」計劃配置與使用之訓練，並因應 貴客戶組織之重要需求；
- IBM Security Resilient 已依據 貴客戶組織特定處理程序，對「教戰手冊」進行配置；
- 如何追蹤依 貴客戶組織之需求與業界實作典範所訂定之 KPI 與測量指標；及
- 指明支援、自動化及精心安排端對端處理程序之整合機會。

1.3.2 IBM SEL for Resilient Premium Starter Service

在 3 日遠端約定中，IBM 將執行下列事項：

- 協助訂定 IBM Security Resilient 架構
- 安裝 IBM Security Resilient（在適用情形下）
- 於 貴客戶環境中起始配置 IBM Security Resilient；及
- 對「分析師」與「設計師」進行 貴客戶現行「事故因應」計劃配置與使用之訓練，並因應 貴客戶組織之重要需求。

1.3.3 IBM SEL for Resilient Additional Day

除 Base 或 Premium Starter 服務以外，於 1 日遠端約定中，IBM 亦會進行事先合意之 IBM Security Resilient 有關活動。例如：

- 進一步支援 IBM Security Resilient 或擴充元件之安裝或配置（在適用情形下）；
- 進一步訓練或支援「分析師」，以確認準備將 IBM Security Resilient 當作 貴客戶重要 SOAR 解決方案之備妥程度；
- 指導「設計師」如何配置及使用其自己的「教戰手冊」，以因應 貴客戶組織之重要需求；或
- 進行 IBM Security Resilient 環境快速掃描，以建議可能改善之處。

2. 資料處理及保護 Data Sheet

「IBM 之資料處理附錄」（網址：http://ibm.com/dpa）(DPA) 及 Data Processing and Protection Data Sheet（稱為 Data Sheet 或「DPA 附件」）（如以下鏈結所示）提供有關「雲端服務」之其他資料保護資訊，以及有關可能處理之「內容」類型、所涉及之處理活動、資料保護特定功能及「內容」保留與歸還相關細節等事宜之選項。若適用 i) 歐洲一般資料保護規章 (EU/2016/679) (GDPR)；或 ii) http://www.ibm.com/dpa/dpl 所載明之其他資料保護法，則於其適用的範圍內，「內容」(Content) 所含個人資料適用前揭 DPA。

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=A47500205B1911E6865BC3F213DB63F7

3. 服務水準及技術支援

3.1 服務水準協定

IBM 為 貴客戶提供下列可用度服務水準協定 (SLA)。 IBM 將就本「雲端服務」累計可用度依最高可適用度進行補償，如下表所示。 可用度百分比之計算方式如下：合約月份中的總分鐘數減去合約月份中「服務停用」之總分鐘數，除以合約月份之總分鐘數。「服務停用」定義、請求的處理及如何洽詢 IBM 有關服務可用度問題，載明於「IBM 雲端服務」支援手冊（網址：https://www.ibm.com/software/support/saas_support_overview.html）。

可用性	扣抵 （每月訂用費用之 %*）
小於 99.9%	2%
小於 99.0%	5%
小於 95.0%	10%

* 訂用費用為請求所主張當月之約定價格。

3.2 技術支援

於 IBM 支援手冊（網址：https://www.ibm.com/support/home/pages/support-guide/）中選取本「雲端服務」，即可找到本「雲端服務」之技術支援（包括支援聯絡人詳細資料、嚴重性層次、可用支援時數、回應時間及其他支援資訊與處理程序）。

4. 計費

4.1 計費度量

本「雲端服務」之計費度量載明於「交易文件」中。

下列計費度量適用於本「雲端服務」：

- 「授權使用者」係指被授權透過任何方法以任何直接或間接方式（例如：透過多工程式、裝置或應用程式伺服器）存取「雲端服務」之特定使用者。
- 「並行使用者」係指於特定時間點同時透過任何方法以任何直接或間接方式（例如：透過多工程式、裝置或應用程式伺服器）存取本「雲端服務」之使用者。 一個人多次同步存取本「雲端服務」，僅計為單一「並行使用者」。
- 「約定」為「雲端服務」有關專業或訓練服務。
- 「項目」係指藉由本「雲端服務」之使用而予以管理、處理或與其相關之特定項目。基於本「雲端服務」之目的，一個「項目」為一個「動作」。「動作」係指本「雲端服務」對其他軟體程式所為編配作業或自動化之要求。

5. 附加條款

於 2019 年 1 月 1 日前簽署之「雲端服務合約」（或性質相當的基本雲端合約），適用 https://www.ibm.com/acs 所載明之條款。

5.1 循規驗證

貴客戶應履行下列事項：i) 持續保留記錄，並在 IBM 認為合理必要情形時，依 IBM 要求而提供記錄及系統工具輸出資料，以利 IBM 及其獨立稽核員驗證 貴客戶是否遵循「本合約」；及 ii) 立即訂購必要授權，並依發票中載明之授權人當時費率支付該等授權所需費用、其他費用與賠償責任。前述循規驗證義務於本「雲端服務」期間及其後二年內有效。

5.2 附加程式授權要件

貴客戶必須取得同等數量與類型之基本「雲端服務」與「附加程式雲端服務」之授權。

5.3 使用限制

每位 貴客戶每月最多上限為進行十萬個「威脅服務」查詢。「客戶」於其「威脅服務」啟動後將構件新增至事故，即可建立「威脅服務」查詢。於前述事故保持開啟及作用中狀態後，每隔二日即自動產生一個新「威脅服務」查詢。

每位 貴客戶每日就每一「授權/並行使用者」最多使用上限為產生一百封通知電子郵件。通知電子郵件由 Resilient 平台依據 貴客戶所控制之配置產生之。

5.4 其他資料處理與保護資訊

為免除疑義，特此指明，IBM Resilient SOAR Platform on Cloud：

- 對處於靜態之「內容」不予加密；
- 其設計目的並非用於處理任何「特種個人資料」；及
- 非必要者，不應於任意文字欄位中輸入個人資料。

所處理之「個人資料」，其加密與類型有關詳細資訊載明於以上第 2 節所述 Data Sheet 之 URL。

6. 優先適用條款

6.1 資料之使用

因 貴客戶使用本「雲端服務」所生結果，如為「客戶內容」（「洞察」）特有的結果或足以識別 貴客戶者，IBM 不予使用或揭露。但 IBM 為改善本「雲端服務」，得使用「內容」及其在提供本「雲端服務」時自「內容」（「洞察」除外）所產生之其他資訊。IBM 基於威脅偵測與保護之目的，亦得分享內嵌於「內容」之威脅識別碼及其他安全資訊。