IBM Security QRadar SIEM
版本 7.2.4

入門手冊

IBM

附註

在使用本資訊及其所支援的產品之前，請閱讀第 21 頁的『聲明』中的資訊。

產品資訊

本文件適用於 IBM QRadar Security Intelligence Platform 7.2.4 版 及後續發行版，直至有本文件的更新版本替代爲止。

目錄

QRadar SIEM 入門簡介

《IBM Security QRadar® SIEM 入門手冊》爲您介紹主要概念、安裝處理程序的概觀，以及您在使用者介面中執行的基本作業。

目標讀者

此資訊旨在供負責調查及管理網路安全的安全管理者使用。 若要使用本手冊，您必須具有公司網路基礎架構與網路技術的知識。

技術說明文件

如需如何存取更多技術說明文件、技術文件及版本注意事項的相關資訊，請參閱存取 IBM® Security 說明文件技術文件 (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861)。

聯絡客戶支援中心

如需聯絡客戶支援中心的相關資訊，請參閱>支援與下載技術文件 (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861)。

良好安全實務的陳述

IT 系統安全涉及透過預防、偵測及回應企業內外的不當存取來保護系統與資訊。不當存取可能導致變更、損壞、不當或誤用資訊，也可能導致損壞或誤用系統，包括用於攻擊其他系統。 沒有任何 IT 系統或產品應該被看作完全安全，且沒有單個產品、服務或安全手段可以完全有效預防不當使用或存取。 IBM 系統、產品及服務設計爲合法的綜合性安全方法的一部分，將需要包含其他作業程序，且可能需要其他系統、產品或服務，才能更爲有效。 IBM 不保證任何系統、產品或服務免於或將讓貴企業免於任何一方的惡意或非法行爲。

請注意：

使用本程式可能會與部分法律或法規相抵觸。包括隱私權、資料保護、僱佣及電子通訊與儲存相關的法律或法規。IBM Security QRadar 必須以合法之目的並透過合法方式使用。客戶同意在遵循適用法律、法規及原則，並承擔所有責任的前提下使用本程式。被授權方代表它將取得或已取得合法使用 IBM Security QRadar 所需的同意、許可權或授權。

第 1 章 QRadar SIEM 概觀

IBM Security QRadar SIEM 是一種網路安全管理平台，提供狀況狀態提示及相符性支援。 QRadar SIEM 會結合使用基於流程的網路知識、安全事件相關性與基於資產的漏洞評量。

若要開始使用本產品，請配置基本 QRadar SIEM 安裝、收集事件及流程資料，以及產生報告。

日誌活動

在 IBM Security QRadar SIEM 中，您可以即時監視及顯示網路事件，或者執行進階搜尋。

日誌活動標籤將事件資訊顯示爲來自某個日誌來源（例如防火牆或路由器裝置）的記錄。使用**日誌活動**標籤，您可以執行下列作業：

- 調查事件資料。
- 即時調查傳送至 QRadar SIEM 的事件日誌。
- 搜尋事件。
- 透過使用可配置的時間序列圖表，來監視日誌活動。
- 識別誤判以調整 QRadar SIEM。

網路活動

在 IBM Security QRadar SIEM 中，您可以調查兩個主機之間的通訊階段作業。

網路活動標籤顯示如何傳播網路資料流量及傳播哪些資料流量（如果已啓用內容擷取選項）的相關資訊。 使用**網路活動**標籤，您可以執行下列作業：

- 即時調查傳送至 QRadar SIEM 的流程。
- 搜尋網路流程。
- 透過使用可配置的時間序列圖表，來監視網路活動。

資產

QRadar SIEM 會透過使用被動流程資料及漏洞資料來自動建立資產設定檔，從而探索網路伺服器和主機。

資產設定檔提供網路中每一個已知資產（包括正在執行的服務）的相關資訊。 資產設定檔資訊用於相關性用途，這可有助於減少誤判。

使用「資產」標籤，您可以執行下列作業：

- 搜尋資產。
- 檢視所有已瞭解的資產。
- 檢視已瞭解資產的識別資訊。
- 調整誤判漏洞。

攻擊

在 IBM Security QRadar SIEM 中，您可以調查攻擊，以判定網路問題的主要原因。

透過使用**攻擊**標籤，您可以檢視網路上發生的所有攻擊，並完成下列作業：

- 調查網路上的攻擊、來源與目的地 IP 位址、網路行爲及異常。
- 建立來自多個網路的事件及流程與同一目的地 IP 位址的關聯。
- 導覽**攻擊**標籤的各頁面，以調查事件與流程詳細資料。
- 判定導致攻擊的唯一事件。

報告

在 IBM Security QRadar SIEM 中，您可以建立自訂報告或使用預設報告。

QRadar SIEM 提供預設報告範本，您可以對其加以自訂、品牌再造並配送給 QRadar SIEM 使用者。

報告範本按報告類型分組，例如相符性、裝置、執行性及網路報告。 使用**報告**標籤完成下列作業：

- 建立、配送及管理 QRadar SIEM 資料的報告。
- 建立自訂報告以用於作業及執行。
- 將安全與網路資訊結合至單一報告。
- 使用或編輯預先安裝的報告範本。
- 使用自訂標誌建立報告品牌。 建立品牌有利於將報告配送給不同的讀者。
- 設定產生自訂及預設報告的排程。
- 以各種格式發佈報告。

資料收集

QRadar SIEM 接受來自許多裝置之各種格式的資訊，其中包括安全事件、網路資料流量及掃描結果。

收集的資料分類爲三個主要區段：事件、流程及漏洞評量資訊。

事件資料收集

事件由下列日誌來源產生：防火牆、路由器、伺服器及侵入偵測系統 (IDS) 或侵入預防系統 (IPS) 等。

大部分日誌來源使用 Syslog 通訊協定，將資訊傳送至 QRadar SIEM。 QRadar SIEM 也支援下列通訊協定：

- 簡易網路管理通訊協定 (SNMP)
- Java™ 資料庫連線功能 (JDBC)
- 安全裝置事件交換 (SDEE)

依預設，QRadar SIEM 在某個特定時間範圍內接收到特定數目的可識別日誌之後，即可自動偵測日誌來源。 順利偵測到日誌來源之後，QRadar SIEM 會將適當的裝置支援模組 (DSM) 新增至「日誌來源」視窗中的**管理**標籤。

雖然大部分 DSM 都包括原生日誌傳送功能，但仍有一些 DSM 需要額外配置及/或代理程式才能傳送日誌。配置會因 DSM 類型不同而異。 您必須確保 DSM 配置爲以 QRadar SIEM 支援的格式傳送日誌。如需配置 DSM 的相關資訊，請參閱 *DSM Configuration Guide*。

某些日誌來源類型（例如路由器及交換器）未傳送足夠的日誌，QRadar SIEM 無法快速偵測及新增它們至「日誌來源」清單。 您可以手動新增這些日誌來源。 如需手動新增日誌來源的相關資訊，請參閱 *Log Sources User Guide*。

收集的資料分類爲三個主要區段：事件、流程及漏洞評量 (VA) 資訊。

流程資料收集

流程提供網路資料流量的相關資訊，且它們可以各種格式（包括 flowlog 檔、NetFlow、J-Flow、sFlow 及 Packeteer）傳送至 QRadar SIEM。

透過同步接受多種流程格式，QRadar SIEM 可以偵測嚴格依賴於事件以取得資訊而可能遺漏的威脅及活動。

QRadar QFlow 收集器 提供完整的網路資料流量應用程式偵測，而無論應用程式作業所在的埠爲何。 例如，如果 Internet Relay Chat (IRC) 通訊協定在埠 7500/TCP 上進行通訊，則 QRadar QFlow 收集器 會將資料流量識別爲 IRC，並提供交談開始時的封包擷取。 NetFlow 及 J-Flow 僅通知您埠 7500/TCP 上有資料流量，而不提供任何有關所使用通訊協定爲何的環境定義。

共用鏡映埠位置包括核心、DMZ、伺服器及應用程式交換器，NetFlow 提供來自邊界路由器及交換器的補充資訊。

QRadar QFlow 收集器 依預設已啓用，且要求鏡映埠、SPAN 埠或分流器連接至 QRadar SIEM 軟體驅動裝置上的可用介面。當鏡映埠連接至 QRadar SIEM 軟體驅動裝置上的其中一個網路介面時，流程分析即會自動開始。依預設，QRadar SIEM 會在管理介面上於埠 2055/UDP 上監視 NetFlow 資料流量。您可以指派額外 NetFlow 埠（如果必要的話）。

漏洞評量資訊

QRadar SIEM 可以從各種協力廠商掃描器匯入漏洞評量資訊。

漏洞評量資訊可協助 QRadar Risk Manager 識別作用中的主機、開啓的埠及潛在的漏洞。

QRadar Risk Manager 使用漏洞評量資訊，對網路上的攻擊量級進行分級。

視漏洞評量掃描器類型而定，QRadar Risk Manager 可以從掃描器伺服器匯入掃描結果，或者從遠端啓動掃描。

QRadar SIEM 規則

規則對事件、流程或攻擊執行測試，且如果符合所有測試條件，則規則會產生回應。

QRadar SIEM 所包含的規則用於偵測各種活動，其中包括過多的防火牆拒絕次數、多次失敗登入嘗試及潛在的殭尸網路活動。 如需規則相關資訊，請參閱 *IBM Security QRadar SIEM Administration Guide*。

下列清單說明兩個規則種類：

- 自訂規則對事件、流程及攻擊執行測試，以偵測網路中的異常活動。
- 異常偵測規則對已儲存的流程或事件搜尋結果執行測試，以偵測網路中何時發生異常資料流量型樣。

重要：具有非管理存取權的使用者可以建立他們可以存取之網路區域的規則。 您必須具有適當的角色權限，才能管理規則。 如需使用者角色權限的相關資訊，請參閱 *IBM Security QRadar SIEM Administration Guide*。

支援的 Web 瀏覽器

若要使 IBM Security QRadar 產品中的功能正常工作，您必須使用支援的 Web 瀏覽器。

當您存取 QRadar 系統時，會提示您輸入使用者名稱與密碼。使用者名稱與密碼必須由管理者事先配置。

下表列出了支援的 Web 瀏覽器版本。

表 1. QRadar 產品支援的 Web 瀏覽器

Web 瀏覽器	受支援的版本
Mozilla Firefox	17.0 延伸支援版 24.0 延伸支援版
已啓用文件模式及瀏覽器模式的 32 位元 Microsoft Internet Explorer	9.0 10
Google Chrome	截至 IBM Security QRadar 7.2.4 版 產品發行之日的現行版本

第 2 章 開始進行 QRadar SIEM 部署

管理者必須先部署 QRadar SIEM，然後才能評估 IBM Security QRadar SIEM 主要功能。

若要部署 QRadar SIEM，管理者必須執行下列作業：

- 安裝 QRadar SIEM 軟體驅動裝置。
- 配置 QRadar SIEM 安裝。
- 收集事件、流程及漏洞評量 (VA) 資料。
- 調整 QRadar SIEM 安裝。

安裝 QRadar SIEM 軟體驅動裝置

管理者必須安裝 QRadar SIEM 軟體驅動裝置，才能存取使用者介面。

開始之前

在安裝 QRadar SIEM 評估軟體驅動裝置之前，確保您具有：

- 可用於包含兩個裝置之軟體驅動裝置的空間。
- 框架滑軌及擱板（已裝載）。
- 選用項目。 用於存取「主控台」的 USB 鍵盤及標準 VGA 顯示器。

程序

1. 將管理網路介面連接至標示爲「乙太網路 1」的埠。
2. 將專用電源接頭插入軟體驅動裝置背面。
3. 如果您需要存取「主控台」，則連接 USB 鍵盤及標準 VGA 顯示器。
4. 如果軟體驅動裝置上有面板， 則向內推任一側的卡舌，並從軟體驅動裝置取下面板，以卸除面板。
5. 開啓軟體驅動裝置的電源。

QRadar SIEM 軟體驅動裝置

QRadar SIEM 評估軟體驅動裝置是一個 2 U 的框架裝載伺服器。 評估設備不提供框架滑軌或擱板。

QRadar SIEM 軟體驅動裝置包括四個網路介面。 針對此評估，使用標示爲「乙太網路 1」的介面作爲管理介面。

您可以將剩餘三個監視介面用於流程收集。 QRadar QFlow 收集器 提供完整網路應用程式分析，並可以在每次交談開始時執行封包擷取。 視 QRadar SIEM 軟體驅動裝置而定，當 SPAN 埠或分流器連接至「乙太網路 1」以外的任何介面時，流程分析會自動開始。可能需要執行額外步驟，才能在 QRadar SIEM 內啓用 QRadar QFlow 收集器 元件。

如需相關資訊，請參閱 *IBM Security QRadar SIEM Administration Guide*。

限制：QRadar SIEM 評估軟體驅動裝置進行流程分析時的限制是 50 Mbps。 請確保在監視介面上進行流程收集時的聚集資料流量不超出 50 Mbps。

QRadar SIEM 配置

透過配置 QRadar SIEM，您可以檢閱網路階層並自訂自動更新項目。

程序

1. 確保下列應用程式安裝在您用來存取 QRadar 產品使用者介面的所有桌面系統上：
   - Java 執行時期環境 (JRE) 1.7 版 或 IBM 64 位元執行時期環境 Java 7.0 版
   - Adobe Flash 10.x 版
2. 確保您正在使用受支援的 Web 瀏覽器。 請參閱第 4 頁的『支援的 Web 瀏覽器』。
3. 如果您使用 Internet Explorer，請啓用文件模式及瀏覽器模式。
   a. 在 Internet Explorer Web 瀏覽器中，按 F12 以開啓「開發者工具」視窗。
   b. 按一下**瀏覽器模式**，並選取 Web 瀏覽器的版本。
   c. 按一下**文件模式**，並選取 **Internet Explorer 7.0 標準**。
4. 透過鍵入下列 URL，登入 QRadar SIEM 使用者介面：

   https://<IP Address>

   其中，<IP Address> 是 QRadar SIEM 主控台 的 IP 位址。

網路階層

您可以檢視按照商業功能組織的不同網路區域，並根據商業價值風險設定威脅及原則資訊的優先順序。

QRadar SIEM 使用網路階層來執行下列作業：

- 瞭解網路資料流量並檢視網路活動。
- 監視網路中的特定邏輯群組或服務，例如市場行銷、DMZ 或 VoIP。
- 監視資料流量，並側寫每一個群組及群組內主機的行爲。
- 判定並識別本端及遠端主機。

爲了進行評估，會併入包含預先定義邏輯群組的預設網路階層。 檢閱網路階層的正確性及完整性。 如果您的環境包括未顯示在預先配置之網路階層中的網路範圍，您必須手動新增它們。

在網路階層中定義的物件無需實際存在於環境中。 隸屬於基礎架構的所有邏輯網路範圍都必須定義爲網路物件。

註：如果您的系統不包括完整的網路階層，則使用**管理**標籤來建立環境特定階層。

如需相關資訊，請參閱 *IBM Security QRadar SIEM Administration Guide*。

檢閱網路階層

您可以檢閱網路階層。

程序

1. 按一下**管理**標籤。
2. 在導覽窗格中，按一下**系統配置**。
3. 按一下**網路階層**圖示。
4. 在**管理群組：頂端**清單中，按一下 **Regulatory_Compliance_Servers**。

   如果網路階層未包括合規性伺服器元件，則可以對此程序的剩餘部分使用「郵件」元件。
5. 按一下**編輯此物件**圖示。
6. 若要新增相符性伺服器：
   a. 在 **IP/CIDR** 欄位中，鍵入相符性伺服器的 IP 位址或 CIDR 範圍。
   b. 按一下**新增**。
   c. 對所有相符性伺服器重複上述步驟。
   d. 按一下**儲存**。
   e. 對您想要編輯的任何其他網路重複此處理程序。
7. 在**管理**標籤功能表上，按一下**部署變更**。

   您可以使用最新的網路安全資訊，來自動或手動更新配置檔。 QRadar SIEM 使用系統配置檔來提供有用的網路資料流程性質。

自動更新

QRadar SIEM 主控台必須連接至網際網路，才能接收更新項目。 如果您的主控台未連接至網際網路，則必須配置內部更新伺服器。

如需設定自動更新伺服器的相關資訊，請參閱 *IBM Security QRadar SIEM 使用手冊*。

使用 QRadar SIEM，您可以取代現有配置檔，或者整合已更新檔案與現有檔案。

軟體更新可以從下列網站進行下載：

http://www.ibm.com/support/fixcentral/

更新檔案可以包括下列更新項目：

- 配置更新項目，其中包括配置檔變更、漏洞、QID 對映及安全威脅資訊更新項目。
- DSM 更新項目，其中包括剖析問題更正項目、掃描器變更及通訊協定更新項目。
- 主要更新項目，其中包括已更新 JAR 檔之類的項目。
- 次要更新項目，其中包括額外線上說明內容或已更新 Script 之類的項目。

配置自動更新設定

您可以自訂 QRadar SIEM 更新項目、更新類型、伺服器配置及備份設定的頻率。

程序

1. 按一下**管理**標籤。
2. 在導覽窗格中，按一下**系統配置**。
3. 按一下**自動更新**圖示。
4. 在導覽窗格中，按一下**變更設定**。

5. 在**自動更新排程**窗格中，接受預設參數。
6. 在**更新類型**窗格中，配置下列參數：
   a. 在**配置更新項目**清單框中，選取**自動更新**。
   b. 接受下列參數的預設值：
      - DSM、掃描器、通訊協定更新項目。
      - 主要更新項目。
      - 次要更新項目。
7. 清除**自動部署**勾選框。

   依預設，會選取該勾選框。 如果未選取該勾選框，則系統通知會顯示在**儀表板**標籤上，指出您必須在安裝更新項目之後部署變更。
8. 按一下**進階**標籤。
9. 在**伺服器配置**窗格中，接受預設參數。
10. 在**其他設定**窗格中，接受預設參數。
11. 按一下**儲存**，並關閉「更新項目」視窗。
12. 在工具列上，按一下**部署變更**。

收集事件

透過收集事件，您可以即時調查傳送至 QRadar SIEM 的日誌。

程序

1. 按一下**管理**標籤。
2. 在導覽窗格中，按一下**資料來源**。
3. 按一下**日誌來源**圖示。
4. 檢閱日誌來源的清單，並對日誌來源進行任何必要的變更。

   如需配置日誌來源的相關資訊，請參閱 *Log Sources User Guide*。
5. 關閉「日誌來源」視窗。
6. 在**管理**標籤功能表上，按一下**部署變更**。

收集流程

透過收集流程，您可以調查主機之間的網路通訊階段作業。

如需如何在協力廠商網路裝置（例如交換器及路由器）上啓用流程的相關資訊，請參閱您的供應商說明文件。

程序

1. 按一下**管理**標籤。
2. 在導覽功能表中，按一下**資料來源 > 流程**。
3. 按一下**流程來源**圖示。
4. 檢閱流程來源的清單，並對流程來源進行任何必要的變更。

   如需配置流程來源的相關資訊，請參閱 *IBM Security QRadar SIEM Administration Guide*。

5. 關閉「流程來源」視窗。
6. 在**管理**標籤功能表上，按一下**部署變更**。

匯入漏洞評量資訊

透過匯入漏洞評量 (VA) 資訊，您可以識別作用中的主機、開啓的埠及潛在的漏洞。

程序

1. 按一下**管理**標籤。
2. 在導覽功能表中，按一下**資料來源 > 漏洞**。
3. 按一下**漏洞評量掃描器**圖示。
4. 在工具列上，按一下**新增**。
5. 輸入參數的值。

   參數取決於您想要新增的掃描器類型。 如需相關資訊，請參閱 *Vulnerability Assessment Configuration Guide*。

   重要：「CIDR 範圍」指定 QRadar SIEM 將哪些網路整合至掃描結果。 例如，如果您想要針對 192.168.0.0/16 網路展開掃描，並指定 192.168.1.0/24 作爲 CIDR 範圍，則只會整合來自 192.168.1.0/24 範圍的結果。
6. 按一下**儲存**。
7. 在**管理**標籤功能表上，按一下**部署變更**。
8. 按一下**排程漏洞評量掃描器**圖示。
9. 按一下**新增**。
10. 指定您想要執行掃描之頻率的準則。

    視掃描類型而定，這包括 QRadar SIEM 匯入掃描結果或啓動新掃描的頻率。 您還必須指定要在掃描結果中包括的埠。
11. 按一下**儲存**。

QRadar SIEM 調整

您可以調整 QRadar SIEM，以符合您環境的需要。

在調整 QRadar SIEM 之前，等待一天以讓 QRadar SIEM 偵測網路上的伺服器、儲存事件及流程，以及建立基於現有規則的攻擊。

管理者可以執行下列調整作業：

- 透過在**日誌活動**及**網路活動**的**快速過濾器**內容上啓用有效負載索引，最佳化事件及流程有效負載搜尋。
- 透過自動或手動新增伺服器至建置區塊，提供更快的起始部署和更簡單的調整。
- 透過建立或修改自訂規則及異常偵測規則，配置對事件、流程及攻擊狀況的回應。
- 確保網路中每一個主機所建立的攻擊都基於最新規則、已探索伺服器及網路階層。

有效負載索引作業

使用在**日誌活動**及**網路活動**標籤上提供的**快速過濾器**功能，來搜尋事件及流程有效負載。

若要最佳化**快速過濾器**，您可以啓用有效負載索引**快速過濾器**內容。

啓用有效負載索引作業可能會降低系統效能。 在**快速過濾器**內容上啓用有效負載索引作業之後，監視索引統計資料。

如需索引管理及統計資料的相關資訊，請參閱 *IBM Security QRadar SIEM Administration Guide*。

啓用有效負載索引作業

您可以透過在**日誌活動**及**網路活動**的**快速過濾器**內容上啓用有效負載索引，最佳化事件及流程有效負載搜尋。

程序

1. 按一下**管理**標籤。
2. 在導覽窗格中，按一下**系統配置**。
3. 按一下**索引管理**圖示。
4. 在**快速搜尋**欄位中，鍵入**快速過濾器**。
5. 按一下您想要編製索引的**快速過濾器**內容。
6. 按一下**啓用索引**。
7. 按一下**儲存**。
8. 按一下**確定**。
9. 選擇性的： 若要停用有效負載索引，請選擇下列其中一個選項：
   - 按一下**停用索引**。
   - 用滑鼠右鍵按一下內容，並從功能表中選取**停用索引**。

下一步

如需「索引管理」視窗中顯示之參數的詳細資訊，請參閱 *IBM Security QRadar SIEM Administration Guide*。

伺服器及建置區塊

QRadar SIEM 會自動探索及分類網路中的伺服器，從而提供更快的起始部署，並在發生網路變更時更簡單地進行調整。

若要確保將適當的規則套用至伺服器類型，您可以新增個別裝置或整個位址範圍內的裝置。您可以手動將不符合唯一通訊協定的伺服器類型輸入至各自的「主機定義建置區塊」中。 例如，將下列伺服器類型新增至建置區塊，可以減少進一步調整誤判的需要：

- 將網路管理伺服器新增至 **BB:HostDefinition：網路管理伺服器**建置區塊。
- 將 Proxy 伺服器新增至 **BB:HostDefinition：Proxy 伺服器**建置區塊。
- 將病毒及 Windows 更新伺服器新增至 **BB:HostDefinition：病毒定義及其他更新伺服器**建置區塊。
- 將「漏洞評量掃描器」新增至 **BB-HostDefinition：漏洞評量掃描器來源 IP** 建置區塊。

「伺服器探索」功能使用資產設定檔資料庫，來探索網路上數個類型的伺服器。 「伺服器探索」功能會列出自動探索到的伺服器，您可以選取想要包括在建置區塊中的伺服器。

如需探索伺服器的相關資訊，請參閱 *IBM Security QRadar SIEM Administration Guide*。

使用建置區塊，您可以在其他規則中重複使用特定規則測試。 您可以透過使用建置區塊來調整 QRadar SIEM 並啓用額外相關性規則，來減少誤判數。

自動新增伺服器至建置區塊

您可以將伺服器自動新增至建置區塊。

程序

1. 按一下**資產**標籤。
2. 在導覽窗格中，按一下**伺服器探索**。
3. 在**伺服器類型**清單中，選取您想要探索的伺服器類型。

   將剩餘參數保留爲預設值。
4. 按一下**探索伺服器**。
5. 在「相符伺服器」窗格中，選取您想要指派給伺服器角色之所有伺服器的勾選框。
6. 按一下**核准選取的伺服器**。

   記住：您可以用滑鼠右鍵按一下任何 IP 位址或主機名稱，以顯示 DNS 解析資訊。

手動新增伺服器至建置區塊

如果未自動偵測到伺服器，您可以手動將該伺服器新增至其對應的「主機定義建置區塊」。

程序

1. 按一下**攻擊**標籤。
2. 在導覽窗格中，按一下**規則**。
3. 在**顯示**清單中，選取**建置區塊**。
4. 在**群組**清單中，選取**主機定義**。

   建置區塊的名稱對應於伺服器類型。 例如，**BB:HostDefinition：Proxy 伺服器**適用於環境中的所有 Proxy 伺服器。
5. 若要手動新增主機或網路，請按兩下適合您環境的對應主機定義建置區塊。
6. 在**建置區塊**欄位中，按一下片語**當來源或目的地 IP 是下列其中一項時**後面畫底線的值。
7. 在**輸入 IP 位址或 CIDR** 欄位中，鍵入您想要指派給建置區塊的主機名稱或 IP 位址範圍。
8. 按一下**新增**。
9. 按一下**提交**。
10. 按一下**完成**。
11. 針對您想要新增的每一個伺服器類型，重複上述步驟。

配置規則

從**日誌活動**、**網路活動**及**攻擊**標籤中，您可以配置規則或建置區塊。

程序

1. 按一下**攻擊**標籤。
2. 按兩下您想要調查的攻擊。
3. 按一下**顯示 > 規則**。
4. 按兩下規則。

   您可以進一步調整規則。 如需調整規則的相關資訊，請參閱 *IBM Security QRadar SIEM Administration Guide*
5. 關閉「規則」精靈。
6. 在「規則」頁面中，按一下**動作**。
7. 選擇性的： 如果您想要防止在超出攻擊保留期間之後將攻擊從資料庫中移除，請選取**保護攻擊**。
8. 選擇性的： 如果您想要將攻擊指派給某個 QRadar SIEM 使用者，請選取**指派**。

相關概念:

第 3 頁的『QRadar SIEM 規則』
規則對事件、流程或攻擊執行測試，且如果符合所有測試條件，則規則會產生回應。

清除 SIM 模型

清除 SIEM 模型，以確保每一個主機所建立的攻擊都基於最新規則、已探索伺服器及網路階層。

程序

1. 按一下**管理**標籤。
2. 在工具列上，選取**進階 > 清除 SIM 模型**。
3. 按一下所需的選項：

   軟清除，可將攻擊設定爲非作用中。

   軟清除配合選用**停用所有攻擊**，可關閉所有攻擊。

   硬清除，可消除所有項目。
4. 按一下**您確定要重設資料模型嗎？**。
5. 按一下**繼續進行**。
6. 完成 SIM 重設處理程序之後，重新整理您的瀏覽器。

結果

當您清除 SIM 模型時，會關閉所有現有攻擊。 清除 SIM 模型不會影響現有事件及流程。

第 3 章 開始使用 QRadar SIEM

若要開始使用 IBM Security QRadar SIEM，請瞭解如何搜尋事件、流程及資產。 同時瞭解如何調查攻擊及建立報告。

例如，您可以透過使用**日誌活動**及**網路活動**標籤中的預設已儲存搜尋，來搜尋資訊。 您也可以建立及儲存您自己的自訂搜尋。

管理者可以執行下列作業：

- 透過使用特定準則來搜尋事件資料，並在結果清單中顯示符合搜尋準則的事件。 選取、組織及分組事件資料的直欄。
- 以視覺化方式即時監視及調查流程資料，或者執行進階搜尋以過濾顯示的流程。 檢視流程資訊，以判定如何傳播網路資料流量，以及傳播哪些網路資料流量。
- 檢視所有已瞭解的資產，或者搜尋環境中的特定資產。
- 調查網路上的攻擊、來源與目的地 IP 位址、網路行爲及異常。
- 編輯、建立、排程及配送預設或自訂報告。

搜尋事件

您可以搜尋 QRadar SIEM 在過去 6 個小時中收到的所有鑑別事件。

程序

1. 按一下**日誌活動**標籤。
2. 在工具列上，選取**搜尋 > 新搜尋**。
3. 在「時間範圍」窗格中，定義事件搜尋的時間範圍：
   a. 按一下**最近**。
   b. 在**最近**清單中，選取**前 6 個小時**。
4. 在「搜尋參數」窗格中，定義搜尋參數：
   a. 在第一個清單中，選取**種類**。
   b. 在第二個清單中，選取**等於**。
   c. 在**高層次種類**清單中，選取**鑑別**。
   d. 在**低層次種類**清單中，接受預設值**任何**。
   e. 按一下**新增過濾器**。
5. 在「直欄定義」窗格的**顯示**清單中，選取**事件名稱**。
6. 按一下**搜尋**。

儲存事件搜尋準則

您可以儲存指定的事件搜尋準則，以供未來使用。

程序

1. 按一下**日誌活動**標籤。
2. 在工具列上，按一下**儲存準則**。

3. 在**搜尋名稱**欄位中，鍵入**範例搜尋 1**。
4. 在「時間範圍選項」窗格中，按一下**最近**。
5. 在**最近**清單中，選取**前 6 個小時**。
6. 按一下**包括在我的快速搜尋中**。
7. 按一下**包括在我的儀表板中**。

   如果未顯示**包括在我的儀表板中**，請按一下**搜尋 > 編輯搜尋**，以驗證您是否在「直欄定義」窗格中選取了**事件名稱**。
8. 按一下**確定**。

下一步

配置時間序列圖表。 如需相關資訊，請參閱『配置時間序列圖表』。

配置時間序列圖表

您可以顯示互動式時間序列圖表，其代表符合特定時間間隔搜尋的記錄。

程序

1. 在圖表標題列中，按一下**配置**圖示。
2. 在**要繪製的值**清單中，選取**目的地 IP（唯一計數）**。
3. 在**圖表類型**清單中，選取**時間序列**。
4. 按一下**擷取時間序列資料**。
5. 按一下**儲存**。
6. 按一下**更新詳細資料**。
7. 過濾您的搜尋結果：
   a. 用滑鼠右鍵按一下您要過濾的事件。
   b. 按一下**基於事件名稱的過濾器為 <Event Name>**。
8. 若要顯示按使用者名稱分組的事件清單，請從**顯示**清單中選取**使用者名稱**。
9. 驗證您的搜尋在**儀表板**標籤上是否可見：
   a. 按一下**儀表板**標籤。
   b. 按一下**新建儀表板**圖示。
   c. 在**名稱**欄位中，鍵入**範例自訂儀表板**。
   d. 按一下**確定**。
   e. 在**新增項目**清單中，選取**日誌活動 > 事件搜尋 > 範例搜尋 1**。

結果

已儲存事件搜尋的結果顯示在「儀表板」中。

搜尋流程

您可以即時搜尋、監視及調查流程資料。

您也可以執行進階搜尋，以過濾顯示的流程。 檢視流程資訊，以判定如何傳播網路資料流量，以及傳播什麼網路資料流量。

程序

1. 按一下**網路活動**標籤。
2. 在工具列上，按一下**搜尋 > 新搜尋**。
3. 在「時間範圍」窗格中，定義流程搜尋時間範圍：
   a. 按一下**最近**。
   b. 在**最近**清單中，選取**前 6 個小時**。
4. 在「搜尋參數」窗格中，定義您的搜尋準則：
   a. 在第一個清單中，選取**流程方向**。
   b. 在第二個清單中，選取**等於**。
   c. 在第三個清單中，選取 **R2L**。
   d. 按一下**新增過濾器**。
5. 在「直欄定義」窗格的**顯示**清單中，選取**應用程式**。
6. 按一下**搜尋**。

結果

會顯示過去 6 個小時中流程方向爲遠端至本端 (R2L) 的所有流程，這些流程按**應用程式名稱**欄位排序。

儲存流程搜尋準則

您可以儲存指定的流程搜尋準則，以供未來使用。

程序

1. 在**網路活動**標籤工具列上，按一下**儲存準則**。
2. 在**搜尋名稱**欄位中，鍵入名稱**範例搜尋 2**。
3. 在**最近**清單中，選取**前 6 個小時**。
4. 按一下**包括在我的儀表板中**及**包括在我的快速搜尋中**。
5. 按一下**確定**。

下一步

建立儀表板項目。 如需相關資訊，請參閱『建立儀表板項目』。

建立儀表板項目

您可以透過使用儲存的流程搜尋準則，來建立儀表板項目。

程序

1. 在**網路活動**工具列上，選取**快速搜尋 > 範例搜尋 2**。
2. 驗證您的搜尋是否包括在「儀表板」中：
   a. 按一下**儀表板**標籤。
   b. 在**顯示儀表板**清單中，選取**範例自訂儀表板**。
   c. 在**新增項目**清單中，選取**流程搜尋 > 範例搜尋 2**。
3. 配置您的儀表板圖表：

a. 按一下**設定**圖示。

b. 使用配置選項，變更已繪製的值、所顯示的物件數目、圖表類型或圖表中顯示的時間範圍。

4. 若要調查圖表中目前顯示的流程，請按一下**在網路活動中檢視**。

結果

「網路活動」頁面會顯示符合時間序列圖表參數的結果。 如需時間序列圖表的相關資訊，請參閱《*IBM Security QRadar SIEM 使用手冊*》。

搜尋資產

當您存取**資產**標籤時，所顯示的「資產」頁面會移入網路中所有已探索的資產。 若要精簡此清單，您可以配置搜尋參數，以僅顯示您想要調查的資產設定檔。

關於這項作業

使用搜尋功能來搜尋主機設定檔、資產及識別資訊。 識別資訊提供更多詳細資料，例如網路上的 DNS 資訊、使用者登入及 MAC 位址。

例如：

程序

1. 按一下**資產**標籤。
2. 在導覽窗格中，按一下**資產設定檔**。
3. 在工具列上，按一下**搜尋 > 新搜尋**。
4. 如果您想要載入已儲存的搜尋，則執行下列步驟：
   a. 選擇性的： 在**群組**清單中，選取您想要顯示在**可用的已儲存搜尋**清單中的資產搜尋群組。
   b. 選擇下列其中一個選項：
      - 在**鍵入已儲存的搜尋或從清單中選取**欄位中，鍵入您想要載入的搜尋名稱。
      - 在**可用的已儲存搜尋**清單中，選取您想要載入的已儲存搜尋。
   c. 按一下**載入**。
5. 在「搜尋參數」窗格中，定義您的搜尋準則：
   a. 在第一個清單中，選取您想要搜尋的資產參數。 例如，**主機名稱**、**漏洞風險分類**或**技術擁有者**。
   b. 在第二個清單中，選取您想要用於搜尋的修飾元。
   c. 在**項目**欄位中，鍵入與搜尋參數相關的特定資訊。
   d. 按一下**新增過濾器**。
   e. 針對您想要新增至搜尋準則的每一個過濾器，重複上述步驟。
6. 按一下**搜尋**。

範例

您會收到通知，說明正在不當利用 CVE ID CVE-2010-000。 若要判定部署中是否有任何主機容易遭到此不當利用的攻擊，請執行下列步驟：

1. 從搜尋參數的清單中，選取**漏洞外部參照**。
2. 選取 **CVE**。
3. 鍵入 2010-000，以檢視容易遭到該特定 CVE ID 攻擊之所有主機的清單。

如需相關資訊，請參閱 Open Source Vulnerability Database 網站 (*http://osvdb.org/*) 及 National Vulnerability Database (*http://nvd.nist.gov/*)。

攻擊調查

使用**攻擊**標籤，您可以調查網路上的攻擊、來源與目的地 IP 位址、網路行爲及異常。

QRadar SIEM 可以建立事件及流程與同一攻擊（最終產生同一網路發生事件）中位於多個網路上之目的地 IP 位址的關聯。 這可讓您有效調查網路中的每一個攻擊。

檢視攻擊

您可以調查網路中的每一個攻擊。

例如，您可以調查網路上的攻擊、來源與目的地 IP 位址、網路行爲及異常。

程序

1. 按一下**攻擊**標籤。
2. 按兩下您想要調查的攻擊。
3. 在工具列上，選取**顯示 > 目的地**。

   您可以調查每一個目的地，以判定目的地是否已受損或表現出可疑行爲。
4. 在工具列上，按一下**事件**。

結果

「事件清單」視窗會顯示與攻擊相關聯的所有事件。 您可以搜尋、排序及過濾這些事件。

範例：啓用 PCI 報告範本

使用**報告**標籤，您可以啓用、停用及編輯報告範本。

在這個入門作業中，您會啓用「支付卡產業 (PCI)」報告範本。

程序

1. 按一下**報告**標籤。
2. 清除**隱藏非作用中報告**勾選框。
3. 在**群組**清單中，選取**相符性 > PCI**。
4. 選取清單上的所有報告範本：
   a. 按一下清單上的第一個報告。
   b. 透過按住 Shift 鍵，並按一下清單上的最後一個報告，來選取所有報告範本。
5. 在**動作**清單中，選取**切換排程**。
6. 存取產生的報告：
   a. 從**產生的報告**直欄中的清單中，選取您想要檢視的報告時間戳記。

b. 在**格式**直欄中，按一下您想要檢視的報告格式圖示。

範例：基於已儲存的搜尋建立自訂報告

您可以透過匯入搜尋或建立自訂準則，來建立報告。

關於這項作業

在這個入門作業中，您會建立基於在第 13 頁的『搜尋事件』中建立之事件及流程搜尋的報告。

程序

1. 按一下**報告**標籤。
2. 在**動作**清單中，選取**建立**。
3. 按**下一步**。
4. 配置報告排程。
   a. 選取**每日**選項。
   b. 選取**「星期一」**、**「星期二」**、**「星期三」**、**「星期四」**及**「星期五」**選項。
   c. 使用清單，選取 **8:00** 及**上午**。
   d. 確保已選取**是 - 手動產生報告**選項。
   e. 按**下一步**。
5. 配置報告佈置：
   a. 在**方向**清單中，選取**橫向**。
   b. 選取含兩個圖表儲存器的佈置。
   c. 按**下一步**。
6. 在**報告標題**欄位中，鍵入**範例報告**。
7. 配置頂端圖表儲存器：
   a. 在**圖表類型**清單中，選取**事件/日誌**。
   b. 在**圖表標題**欄位中，鍵入**範例事件搜尋**。
   c. 在**將事件/日誌限制為前幾個**清單中，選取 **10**。
   d. 在**圖形類型**清單中，選取**堆疊長條圖**。
   e. 按一下**前 24 個小時的所有資料**。
   f. 在**此事件報告的基礎**清單中，選取**範例搜尋 1**。

      會使用「範例搜尋 1」已儲存搜尋的設定自動將內容移入剩餘參數中。
   g. 按一下**儲存儲存器詳細資料**。
8. 配置底端圖表儲存器：
   a. 在**圖表類型**清單中，選取**流程**。
   b. 在**圖表標題**欄位中，鍵入**範例流程搜尋**。
   c. 在**將流程限制為前幾個**清單中，選取 **10**。
   d. 在**圖形類型**清單中，選取**堆疊長條圖**。
   e. 按一下**前 24 個小時的所有資料**。
   f. 在**可用的已儲存搜尋**清單中，選取**範例搜尋 2**。

會使用「範例搜尋 2」已儲存搜尋的設定自動將內容移入剩餘參數中。

g. 按一下**儲存儲存器詳細資料**。

9. 按**下一步**。
10. 按**下一步**。
11. 選擇報告格式：
    a. 按一下 **PDF 及 HTML** 勾選框。
    b. 按**下一步**。
12. 選擇報告配送通道：
    a. 按一下**報告主控台**。
    b. 按一下**電子郵件**。
    c. 在**輸入報告目的地電子郵件位址**欄位中，鍵入您的電子郵件位址。
    d. 按一下**包括報告作為附件**。
    e. 按**下一步**。
13. 完成最終「報告」精靈詳細資料：
    a. 在**報告說明**欄位中，鍵入範本的說明。
    b. 按一下**是 - 在精靈完成時執行此報告**。
    c. 按一下**完成**。
14. 使用**產生的報告**直欄中的清單框，選取報告的時間戳記。

聲明

本資訊係針對 IBM 在美國所提供之產品與服務所開發。

在其他國家或地區中，IBM 不見得有提供本文件所提及之各項產品、服務或功能。請洽詢當地的 IBM 業務代表，以取得當地目前提供的產品和服務之相關資訊。 這份文件在提及 IBM 的產品、程式或服務時，不表示或暗示只能使用 IBM 產品、程式或服務。只要未侵犯 IBM 之智慧財產權，任何功能相當之產品、程式或服務皆可取代 IBM 之產品、程式或服務。 不過，任何非 IBM 之產品、程式或服務，使用者必須自行負責作業之評估和驗證責任。

本文件所說明之主題內容，IBM 可能擁有其專利或專利申請案。提供本文件不代表授予這些專利的授權。 您可以書面提出授權查詢，來函請寄到：

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

如果是有關雙位元組字集 (DBCS) 資訊的授權查詢，請洽詢所在國的 IBM 智慧財產部門，或書面提出授權查詢，來函請寄到：

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

下段對英國或任何對這些規定與當地法律不一致的其他國家或地區不適用：

IBM 僅以「現狀」提供本書，而不提供任何明示或默示之保證 (包括但不限於可售性或符合特定效用的保證)。 有些地區在特定交易上，不允許排除明示或暗示的保證，因此，這項聲明不一定適合您。

本資訊中可能會有技術上或排版印刷上的訛誤。 因此，IBM 會定期修訂；並將修訂後的內容納入新版中。 IBM 隨時會改進及/或變更本出版品所提及的產品及/或程式，不另行通知。

本資訊中任何對非 IBM 網站的敘述僅供參考，IBM 對該網站並不提供保證。 這些網站中的教材不屬於此 IBM 產品的相關教材，用戶使用這些網站時應自行承擔風險。

IBM 得以各種 IBM 認爲適當的方式使用或散布 貴客戶提供的任何資訊，而無需對 貴客戶負責。

如果本程式之獲授權人爲了 (i) 在個別建立的程式和其他程式（包括本程式）之間交換資訊，以及 (ii) 相互使用所交換的資訊，因而需要相關的資訊，請洽詢：

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

這些資訊可依適當條款而取得，在某些情況下必須付費方得使用。

IBM 基於 IBM 客戶合約、IBM 國際程式授權合約或雙方之任何同等合約的條款，提供本文件所提及的授權程式與其所有適用的授權資料。

本文件中所含的任何效能資料是在控制環境中得出。 因此，在其他作業環境中獲得的結果可能有明顯的差異。 在開發層次的系統上可能有做過一些測量，但不保證這些測量在市面上普遍發行的系統上有相同的結果。 再者，有些測定可能是透過推測方式來評估。實際結果可能不同。 本文件的使用者應驗證其特定環境適用的資料。

本書所提及之非 IBM 產品資訊，取自產品的供應商，或其發佈的聲明或其他公開管道。IBM 並未測試過這些產品，也無法確認這些非 IBM 產品的執行效能、相容性或任何對產品的其他主張是否完全無誤。 有關非 IBM 產品的性能問題應直接洽詢該產品供應商。

有關 IBM 未來動向的任何陳述，僅代表 IBM 的目標和目的而已，並可能於未事先聲明的情況下有所變動或撤回。

所有 IBM 價格爲 IBM 之建議零售價，可隨時更改而不另行通知。 經銷商之價格可與此不同。

本資訊含有日常業務運作所用的資料和報告範例。 爲求儘可能地完整說明，範例包括了個人、公司、品牌和產品的名稱。 所有這些名稱都是虛構的，如有任何類似實際企業所用的名稱及地址之處，純屬巧合。

若貴客戶正在閱讀本項資訊的電子檔，可能不會有照片和彩色說明。

商標

IBM、IBM 標誌及 ibm.com® 是國際商業機器股份有限公司 (IBM) 在美國及/或其他國家或地區的商標或註冊商標。 如果這些及其他 IBM 註冊術語在本資訊中第一次出現時以商標符號（® 或 ™）標示，則這些符號指出發佈本資訊時，IBM 擁有的美國註冊或普通法商標。 此類商標也可能是在其他國家或地區的註冊或普通法商標。 IBM 商標的最新清單可在 Web 的 Copyright and trademark information (www.ibm.com/legal/copytrade.shtml) 中找到。

Java 及所有基於 Java 的商標及標誌是 Sun Microsystems, Inc. 在美國及/或其他國家或地區的商標或註冊商標。

Microsoft、Windows、Windows NT 及 Windows 標誌是 Microsoft Corporation 在美國及/或其他國家或地區的商標。

其他公司、產品及服務名稱可能是第三方的商標或服務標記。

隱私權條款考量

IBM 軟體產品（包括作爲服務解決方案的軟體，即「軟體產品與服務」）可能使用 Cookie 或其他技術來收集產品使用資訊，以有助於改善一般使用者體驗、自訂與一般使用者的互動或爲了其他目的。 在許多情況下，「軟體供應項目」不會收集任何個人識別資訊。 我們的部分「軟體供應項目」有助於讓您能收集個人識別資訊。 如果此「軟體供應項目」使用 Cookie 來收集個人識別資訊，則以下提出此供應項目使用 Cookie 的相關資訊。

視部署的配置而定，「軟體產品與服務」可能使用階段作業 Cookie 收集每個使用者的階段作業 ID，用於階段作業管理和鑑別。 這些 Cookie 可以停用，但是這也將刪除它們啓用的功能。

如果爲此「軟體供應項目」部署的配置讓您的客戶能夠透過 Cookie 及其他技術，從一般使用者收集個人識別資訊，則應該探查適用於此類資料收集之任何法律的您自己的合法建議，其中包括通知及同意的任何需求。

如需針對這些目的的各種技術（其中包括 Cookie）的使用的相關資訊，請參閱 Cookies, Web Beacons and Other Technologies 中的 IBM 的隱私權原則（網址爲 http://www.ibm.com/privacy ），以及 IBM 的線上隱私權條款（網址爲 http://www.ibm.com/privacy/details），以及「IBM 軟體產品及軟體作爲服務隱私權條款」（網址爲 http://www.ibm.com/software/info/product-privacy）。

名詞解釋

本名詞解釋提供 IBM Security QRadar SIEM 軟體及產品的術語和定義。

本名詞解釋中使用下列交互參照：

- *請參閱* 引導您從非偏好的術語參照到偏好的術語，或從縮寫參照到拼出的格式。
- *另請參閱* 讓您參照相關或對照術語。

如需其他術語和定義，請參閱 IBM Terminology 網站（在新視窗中開啓）。

『三劃』 『四劃』 『五劃』 第 26 頁的『六劃』 第 26 頁的『七劃』 第 26 頁的『八劃』 第 26 頁的『九劃』 第 26 頁的『十劃』 第 27 頁的『十一劃』 第 27 頁的『十二劃』 第 28 頁的『十三劃』 第 28 頁的『十四劃』 第 29 頁的『十七劃』 第 29 頁的『十八劃』 第 29 頁的『十九劃』 第 29 頁的『A』 第 29 頁的『C』 第 29 頁的『D』 第 29 頁的『F』 第 29 頁的『H』 第 30 頁的『I』 第 30 頁的『L』 第 30 頁的『M』 第 30 頁的『N』 第 30 頁的『O』 第 30 頁的『Q』 第 30 頁的『R』 第 30 頁的『S』 第 30 頁的『T』 第 30 頁的『W』

三劃

子搜尋 (sub-search)
可在一組完成的搜尋結果中執行搜尋查詢的功能。

子網路 (subnet)
請參閱子網路 (subnetwork)。

子網路 (subnetwork, subnet)
分爲較小的獨立子群組，但仍然交互連接的網路。

子網路遮罩 (subnet mask)
對於網際網路子網路，32 位元遮罩用於識別 IP 位址的主機部分中的子網路位址位元。

四劃

日誌來源 (log source)
產生事件日誌的安全設備或網路設備。

日誌來源延伸 (log source extension)
包含識別及分類事件內容之事件所需的所有正規表示式型樣的 XML 檔。

內容擷取 (content capture)
用於擷取可配置的有效負載量，然後將資料儲存在流程日誌中的處理程序。

五劃

本端到本端 (Local To Local, L2L)
與從一個本端網路到另一個本端網路的內部資料流量相關。

本端到遠端 (Local To Remote, L2R)
與從一個本端網路到另一個遠端網路的內部資料流量相關。

可靠性 (credibility)
0-10 之間的數值比率，用於判定事件或攻擊的完整性。在多個來源報告相同事件或攻擊時，可靠性會增加。

用戶端 (client)
用於要求伺服器提供服務的軟體程式或電腦。

外部掃描裝置 (external scanning appliance)
連接至網路，以收集網路中資產的相關漏洞資訊的機器。

主要 HA 主機 (primary HA host)
連接至 HA 叢集的主要電腦。

主控台 (console)
操作員可以從中控制及觀察系統作業的顯示站。

主機環境定義 (host context)
用於監視元件的服務，以確保每個元件如預期般運作。

加密 (encryption)
在電腦安全中，此處理程序用於將資料轉換爲無法辨識的格式，從而原始資料無法取得，或只能使用解密處理程序取得。

六劃

共用漏洞評分系統 (Common Vulnerability Scoring System, CVSS)
測量漏洞嚴重性的評分系統。

有效負載資料 (payload data)
包含在 IP 流程中的應用程式資料（除了標頭及管理資訊以外）。

自主系統號碼 (autonomous system number, ASN)
在 TCP/IP 中，是指由指派 IP 位址的相同管理中心指派給自主系統的號碼。自主系統號碼可讓自動遞送演算法識別自主系統。

行為 (behavior)
作業或事件的可觀察效果，包括其結果。

次要 HA 主機 (secondary HA host)
連接至 HA 叢集的待命電腦。如果主要 HA 主機失敗，次要 HA 主機會承擔主要 HA 主機的責任。

七劃

攻擊 (offense)
爲回應監視的條件傳送的訊息或產生的事件。例如，攻擊將提供原則是否已違背或網路是否正遭受攻擊的相關資訊。

作用中的系統 (active system)
在高可用性 (HA) 叢集中，是指具有所有正在執行的服務的系統。

位址解析通訊協定 (Address Resolution Protocol, ARP)
用於將 IP 位址自動對映至區域網路中的網路配接卡位址的通訊協定。

身分 (identity)
來自資料來源的屬性集合，代表個人、組織、位置或項目。

系統視圖 (system view)
以視覺方式呈現組成系統的主要及受管理主機。

完整網域名稱 (fully qualified domain name, FQDN)
在網際網路通訊中，是指主機系統的名稱，包括網域名稱的所有子名稱。例如，完整網域名稱爲 rchland.vnet.ibm.com。

完整網路名稱 (fully qualified network name, FQNN)
在網路階層中，是指包括所有部門的物件名稱。例如，完整的網路名稱爲 CompanyA.Department.Marketing。

八劃

金鑰檔 (key file)
在電腦安全中，包含公開金鑰、私密金鑰、信任憑證及證書的檔案。

九劃

相關性 (relevance)
網路上事件、種類或攻擊的相對影響測量。

重新整理計時器 (refresh timer)
手動或定時自動觸發的內部裝置，用於更新現行網路活動資料。

重複的流程 (duplicate flow)
從不同流程來源收到的相同資料傳輸的多個實例。

信任儲存庫檔案 (truststore file)
包含信任實體之公開金鑰的金鑰資料庫檔。

侵入偵測系統 (intrusion detection system, IDS)
此軟體用於偵測對屬於網路或主機系統一部分的受監視資源的嘗試攻擊或成功攻擊。

侵入預防系統 (intrusion prevention system, IPS)
用於嘗試拒絕潛在惡意活動的系統。拒絕機制可能涉及過濾、追蹤或設定速率限制。

待命系統 (standby system)
在作用中的系統失敗時，會自動變成作用中的系統。如果已啓用磁碟抄寫，則會從作用中的系統抄寫資料。

級別 (magnitude)
特定攻擊的相對重要性的測量。級別是根據相關性、嚴重性及可靠性計算的加權值。

十劃

高可用性 (high availability, HA)
與叢集系統相關，該系統會在節點或常駐程式失敗時進行重新配置，以便工作量可以重新配送至叢集中的剩餘節點。

剖析順序 (parsing order)
使用者可定義日誌來源（共用一般 IP 位址或主機名稱）之重要性順序的日誌來源定義。

流程 (flow)
在交談期間透過鏈結傳遞的單一資料傳輸。

流程日誌 (flow log)
流程記錄的集合。

流程來源 (flow sources)
從中擷取流程的來源。流程來源在流程來自受管理主機上安裝的硬體時分類爲內部，在流程傳送至流程收集器時分類爲外部。

通訊協定 (protocol)
一組規則，用於控制通訊網路中兩個以上裝置或系統之間的資料通訊及傳送。

十一劃

規則 (rule)
一組條件式陳述式，可讓電腦系統識別關係及相應地執行自動回應。

掃描器 (scanner)
搜尋 Web 應用程式內的軟體漏洞的自動化安全程式。

勘察 (recon)
請參閱勘察。

勘察 (reconnaissance, recon)
收集網路資源身分相關資訊的方法。可以使用網路掃描及其他技術來編譯網路資源事件清單，然後向其指派嚴重性層次。

區域網路 (local area network, LAN)
用於連接限制區域（如單一大廈或校園）中的數個裝置且可以連接至更大網路的網路。

異常 (anomaly)
與網路預期行爲的偏差。

累計器 (accumulator)
一種暫存器，某運算的一個運算元可以儲存在其中，隨後該運算的結果會取代此運算元。

動態主機配置通訊協定 (Dynamic Host Configuration Protocol, DHCP)
用於集中管理配置資訊的通訊協定。例如，DHCP 會自動將 IP 位址指派給網路中的電腦。

參照表 (reference table)
此表格中的資料記錄將已指派類型的索引鍵對映至其他索引鍵，然後再對映至單個值。

參照集 (reference set)
從網路上的事件或流程衍生的單個元素的清單。例如，IP 位址清單，或者使用者名稱清單。

參照對映 (reference map)
將索引鍵直接對映至值的資料記錄，例如，將使用者名稱對映至廣域 ID。

參照對映集 (reference map of sets)
將一個索引鍵對映至多個值的資料記錄。例如，將特許使用者的清單對映至一個主機。

十二劃

報告 (report)
在查詢管理中，執行查詢及將格式套用至其中所產生的格式化資料。

報告間隔 (report interval)
可配置的時間間隔，在此間隔結束時，事件處理器必須將所有擷取的事件及流程資料傳送至主控台。

葉節點 (leaf)
在樹狀結構中，是指沒有子項的項目或節點。

開放式系統互連 (OSI)
符合用於交換資訊的「國際標準組織 (ISO)」的標準之開放式系統互聯。

開放程式碼漏洞資料庫 (Open Source Vulnerability Database, OSVDB)
由網路安全社群建立的開放程式碼資料庫，可提供有關網路安全漏洞的技術資訊。

違規 (violation)
略過或違反公司原則的動作。

無類別內部網域遞送 (Classless Inter-Domain Routing, CIDR)
用於新增類別 C「網際網路通訊協定 (IP)」位址的方法。這些位址提供給「網際網路服務供應商 (ISP)」來供客戶使用。CIDR 位址可減少遞送表的大小，並使更多 IP 位址在組織內可用。

十三劃

遠端到本端 (Remote To Local, R2L)
從遠端網路至本端網路的外部資料流量。

遠端到遠端 (Remote To Remote, R2R)
從某個遠端網路至另一個遠端網路的外部資料流量。

閘道 (gateway)
用於連接具有不同網路架構的網路或系統的裝置或程式。

傳輸控制通訊協定 (Transmission Control Protocol, TCP)
網際網路及任何遵循用於網際網路通訊協定的「網際網路工程工作小組 (IETF)」標準中使用的通訊協定。TCP 在封包交換的通訊網路及此類網路的交互連接系統中提供了可靠的主機對主機通訊協定。另請參閱網際網路通訊協定 (Internet Protocol)。

遞送規則 (routing rule)
一種條件，在事件資料滿足其準則時，會執行條件及隨後遞送的集合。

資料庫葉節點物件 (database leaf object)
資料庫階層中的終端機物件或節點。

資料點 (datapoint)
復原點的度量值的計算值。

資產 (asset)
已部署或想要在作業環境中部署的可管理物件。

裝置支援模組 (Device Support Module, DSM)
一個配置檔，用於剖析從多個日誌來源接收的事件，及將它們轉換爲可作爲輸出顯示的標準分類架構格式。

十四劃

輕量型目錄存取通訊協定 (Lightweight Directory Access Protocol, LDAP)
一種開放式通訊協定，它使用 TCP/IP 來提供支援 X.500 模型的目錄的存取權，且不會招致更複雜的 X.500「目錄存取通訊協定 (DAP)」的資源需求。例如，您可以使用 LDAP 在網際網路或內部網路目錄中尋找人員、組織及其他資源。

對映參照圖 (reference map of maps)
將兩個索引鍵對映至多個值的資料記錄。例如，將應用程式的位元組總數對映至來源 IP。

管理共用 (administrative share)
對無管理專用權的使用者隱藏的網路資源。管理共用爲管理者提供網路系統上所有資源的存取權。

誤判 (false positive)
歸類爲使用者決定有侵害攻擊的測試結果（指出網站容易遭到攻擊）實際上無侵害攻擊（不是漏洞）。

認證 (credential)
用於授與使用者或處理程序特定存取權的資訊集。

端點 (endpoint)
環境中 API 或服務的位址。API 公開端點，並且同時呼叫其他服務的端點。

漏洞 (vulnerability)
作業系統、系統軟體或應用軟體元件內的安全曝光。

實時掃描 (live scan)
可根據階段作業名稱從掃描結果中產生報告資料的漏洞掃描。

網址轉換 (Network Address Translation, NAT)
在防火牆中，是指將安全的「網際網路通訊協定 (IP)」位址轉換爲外部登錄的位址。這樣可與外部網路進行通訊，但會遮罩在防火牆內使用的 IP 位址。

網域名稱系統 (Domain Name System, DNS)
用於將網域名稱對映至 IP 位址的分散式資料庫系統。

網路加權 (network weight)
套用至每個網路的數值，表示網路的重要性。網路加權由使用者定義。

網路物件 (network object)
網路階層的元件。

網路階層 (network hierarchy)
一種儲存器類型，是網路物件的階層式集合。

網路層 (network layer)
在 OSI 架構中，是指提供服務的層，可在具有可預期服務品質的開放式系統之間建立路徑。

網際網路服務供應商 (Internet service provider, ISP) 可提供網際網路存取權的組織。

網際網路通訊協定 (Internet Protocol, IP)
用於透過網路或互聯網路遞送資料的通訊協定。此通訊協定用作較高通訊協定層與實體網路之間的媒介。另請參閱傳輸控制通訊協定 (Transmission Control Protocol)。

網際網路控制訊息通訊協定 (Internet Control Message Protocol, ICMP)
閘道使用的網際網路通訊協定，用於與來源主機通訊，例如，報告資料包中的錯誤。

十七劃

聯合間隔 (coalescing interval)
組合事件的間隔。以 10 秒鐘間隔進行事件組合，且以與任何目前聯合事件不相符的第一個事件開始。在聯合間隔內，前三個相符事件會組合及傳送至事件處理器。

應用程式簽章 (application signature)
唯一性質集，由封包有效負載的檢查衍生，然後用於識別特定的應用程式。

十八劃

轉遞目的地 (forwarding destination)
用於從日誌來源及流程來源接收原始和正規化資料的一個以上供應商系統。

叢集虛擬 IP 位址 (cluster virtual IP address)
在主要或次要主機與 HA 叢集之間共用的 IP 位址。

簡易網路管理通訊協定 (Simple Network Management Protocol, SNMP)
一組通訊協定，用於監視複式網路中的系統及裝置。在「管理資訊庫 (MIB)」中定義及儲存受管理裝置的相關資訊。

雜湊型訊息鑑別碼 (Hash-Based Message Authentication Code, HMAC)
使用加密的雜湊函數及秘密金鑰的加密碼。

離站目標 (offsite target)
遠離主要站台的裝置，用於從事件收集器接收事件或資料流程。

離站來源 (offsite source)
遠離主要站台的裝置，用於將正規化資料轉遞至事件收集器。

十九劃

嚴重性 (severity)
來源對目的地導致的相關威脅測量。

A

ARP 重新導向 (ARP Redirect)
在網路存在問題時，通知主機的一種 ARP 方法。

ARP 請參閱位址解析通訊協定 (Address Resolution Protocol)。

ASN 請參閱自主系統號碼 (autonomous system number)。

C

CIDR 請參閱無類別內部網域遞送 (Classless Inter-Domain Routing)。

CVSS 請參閱共用漏洞評分系統 (Common Vulnerability Scoring System)。

D

DHCP 請參閱動態主機配置通訊協定 (Dynamic Host Configuration Protocol)。

DNS 請參閱網域名稱系統 (Domain Name System)。

DSM 請參閱裝置支援模組 (Device Support Module)。

F

FQDN 請參閱完整網域名稱 (fully qualified domain name)。

FQNN 請參閱完整網路名稱 (fully qualified network name)。

H

HA 叢集 (HA cluster)
由主要伺服器及一個次要伺服器組成的高可用性配置。

HA 請參閱高可用性。

HMAC 請參閱雜湊型訊息鑑別碼 (Hash-Based Message Authentication Code)。

I

ICMP 請參閱網際網路控制訊息通訊協定 (Internet Control Message Protocol)。

IDS 請參閱侵入偵測系統 (intrusion detection system)。

IP 多重播送 (IP multicast)
將「網際網路通訊協定 (IP)」資料包傳輸至系統集，以形成單一多重播送群組。

IP 請參閱網際網路通訊協定 (Internet Protocol)。

IPS 請參閱侵入預防系統 (intrusion prevention system)。

ISP 請參閱網際網路服務供應商 (Internet service provider)。

L

L2L 請參閱本端到本端 (Local To Local)。

L2R 請參閱本端到遠端 (Local To Remote)。

LAN 請參閱區域網路 (local area network)。

LDAP 請參閱輕量型目錄存取通訊協定 (Lightweight Directory Access Protocol)。

M

Magistrate
用於根據定義的自訂規則分析網路資料流量及安全事件的內部元件。

N

NAT 請參閱網址轉換 (Network Address Translation)。

NetFlow
用於監視網路資料流量流程資料的 Cisco 網路通訊協定。NetFlow 資料包括用戶端和伺服器資訊、使用的埠，以及透過連接至網路的交換器和路由器流動的位元組和封包數目。資料傳送至進行資料分析的 NetFlow 收集器。

O

OSI 請參閱開放式系統互連 (open systems interconnection)。

OSVDB
請參閱開放程式碼漏洞資料庫 (Open Source Vulnerability Database)。

Q

QID 對映 (QID Map)
此分類架構用於識別每個唯一的事件，及將事件對映至低階和高階種類，以判定應關聯和組織事件的方式。

R

R2L 請參閱遠端到本端 (Remote To Local)。

R2R 請參閱遠端到遠端 (Remote To Remote)。

S

SNMP 請參閱簡易網路管理通訊協定 (Simple Network Management Protocol)。

SOAP 一種輕量型 XML 型通訊協定，用於在非集中的分散式環境中交換資訊。SOAP 可以用於查詢及傳回資訊，及呼叫網際網路中的服務。

superflow
包含多個具有類似內容之流程，以透過減少儲存體限制來增加處理容量的單一流程。

T

TCP 請參閱傳輸控制通訊協定 (Transmission Control Protocol)。

W

whois 伺服器 (whois server)
用於擷取已登錄網際網路資源的相關資訊（如網域名稱及 IP 位址配置）的伺服器。

索引

索引順序以中文字，英文字，及特殊符號之次序排列。

Q

S

W