IBM Security QRadar

版本 7.2.6

使用手冊

IBM

附註

在使用本資訊及其所支援的產品之前，請閱讀第 211 頁的『聲明』中的資訊。

產品資訊

本文件適用於 IBM QRadar Security Intelligence Platform 7.2.6 版 及後續發行版，直至由本文件的更新版本替代爲止。

目錄

關於本手冊 ix

第 1 章 QRadar 7.2.6 版 中的使用者新增功能 1

第 2 章 關於 QRadar SIEM 5

安全智慧產品中的功能 5
支援的 Web 瀏覽器 6
在 Internet Explorer 中啓用文件模式和瀏覽器模式 7
IBM Security QRadar 登入 7
RESTful API 7
使用者介面標籤 9
儀表板標籤 9
攻擊標籤 9
日誌活動標籤 9
網路活動標籤 9
資產標籤 9
報告標籤 10
IBM Security QRadar Risk Manager 10
管理標籤 10
QRadar 一般程序 10
檢視訊息 11
排序結果 12
重新整理與暫停使用者介面 12
調查 IP 位址 13
調查使用者名稱 14
系統時間 15
更新使用者喜好設定 15
存取線上說明 16
調整直欄大小 16
[redacted]面大小 16

第 3 章 儀表板管理 17

預設儀表板 17
自訂儀表板 17
自訂儀表板 17
流程搜尋 18
攻擊 18
日誌活動 19
最新報告 19
系統摘要 20
風險監視儀表板 20
監視原則合規性 20
監視風險變更 22
漏洞管理項目 22
系統通知 23
網際網路威脅資訊中心 24
建立自訂儀表板 24
使用儀表板來調查日誌或網路活動 24
配置圖表 25
移除儀表板項目 26
分離儀表板項目 26

重新命名儀表板 26
刪除儀表板 27
管理系統通知 27
將搜尋型儀表板項目新增至新增項目清單 27

第 4 章 攻擊管理 29
攻擊概觀 29
攻擊許可權考量 29
重要詞彙 29
攻擊保留 30
攻擊監視 30
監視「所有攻擊」或「我的攻擊」頁面 30
監視依種類分組的攻擊 31
監視依來源 IP 分組的攻擊 31
監視依目的地 IP 分組的攻擊 32
監視依網路分組的攻擊 32
攻擊管理作業 33
新增附註 33
隱藏攻擊 34
顯示隱藏的攻擊 34
關閉攻擊 34
保護攻擊 35
解除保護攻擊 36
匯出攻擊 36
將攻擊指派給使用者 37
傳送電子郵件通知 37
將項目標示爲追蹤 38
攻擊標籤工具列功能 39
攻擊參數 42

第 5 章 日誌活動調查 63
日誌活動標籤概觀 63
日誌活動標籤工具列 63
右鍵功能表選項 67
狀態列 67
日誌活動監視 67
檢視串流事件 67
檢視正規化事件 68
檢視未處理的事件 70
檢視分組事件 71
事件詳細資料 75
事件詳細資料工具列 77
檢視關聯的攻擊 78
修改事件對映 78
調整誤判 79
PCAP 資料 80
顯示 PCAP 資料直欄 80
檢視 PCAP 資訊 81
將 PCAP 檔案下載至桌面系統 82
匯出事件 82

第 6 章 網路活動調查 85
網路標籤概觀 85
網路活動標籤工具列 85
右鍵功能表選項 87
狀態列 88

溢位記錄 88
網路活動監視 88
檢視串流流程 88
檢視正規化流程 89
檢視分組流程 91
流程詳細資料 94
流程詳細資料工具列 97
調整誤判 97
匯出流程 98

第 7 章 資產管理 99
資產資料的來源 99
送入的資產資料的工作流程 100
資產資料更新 101
資產核對排除規則 101
範例：經調整將 IP 位址排除在黑名單外的資產排除規則 102
資產合併 103
識別資產成長偏差 104
指出資產成長偏差的系統通知 104
範例：日誌來源延伸的配置錯誤會如何導致資產成長偏差 105
疑難排解超出正常大小臨界值的資產設定檔 105
新的資產資料已新增至資產黑名單 106
資產黑名單和白名單 106
資產黑名單 106
資產白名單 107
資產設定檔頁面參數 108
資產設定檔 108
漏洞 108
資產標籤概觀 109
資產標籤清單 109
右鍵功能表選項 110
檢視資產設定檔 111
新增或編輯資產設定檔 113
搜尋資產設定檔 116
儲存資產搜尋準則 118
資產搜尋群組 118
檢視搜尋群組 118
建立新搜尋群組 119
編輯搜尋群組 119
將已儲存的搜尋複製到另一個群組 120
移除群組或從群組移除已儲存的搜尋 120
資產設定檔管理作業 120
刪除資產 121
匯入資產設定檔 121
匯出資產 121
研究資產漏洞 122

第 8 章 圖表管理 125
圖表管理 125
時間序列圖表概觀 125
圖表圖註 126
配置圖表 127

第 9 章 資料搜尋 129
事件和流程搜尋 129
搜尋符合準則的項目 129

儲存搜尋準則 . . . 133
排程搜尋 . . . 134
進階搜尋選項 . . . 135
AQL 搜尋字串範例 . . . 136
「快速過濾器」搜尋選項 . . . 140
攻擊搜尋 . . . 142
在「我的攻擊」和「所有攻擊」頁面上搜尋攻擊 . . . 142
在「依來源 IP」頁上搜尋攻擊 . . . 147
在「依目的地 IP」頁上搜尋攻擊 . . . 148
在「依網路」頁上搜尋攻擊 . . . 149
儲存**攻擊**標籤上的搜尋準則 . . . 150
刪除搜尋準則 . . . 151
使用子搜尋來細化搜尋結果 . . . 151
管理搜尋結果 . . . 152
取消搜尋 . . . 152
刪除搜尋 . . . 153
管理搜尋群組 . . . 153
檢視搜尋群組 . . . 153
建立新的搜尋群組 . . . 154
編輯搜尋群組 . . . 155
將已儲存的搜尋複製到其他群組 . . . 155
移除群組或從群組移除已儲存的搜尋 . . . 155

第 10 章 自訂事件和流程內容 . . . 157
所需許可權 . . . 157
自訂內容類型 . . . 157
建立 Regex 型自訂內容 . . . 158
建立計算型自訂內容 . . . 159
修改自訂內容 . . . 161
複製自訂內容 . . . 162
刪除自訂內容 . . . 162

第 11 章 規則管理 . . . 165
規則許可權考量 . . . 165
規則概觀 . . . 165
規則種類 . . . 165
規則類型 . . . 166
規則條件 . . . 166
規則回應 . . . 167
檢視規則 . . . 168
建立規則 . . . 168
建立異常偵測規則 . . . 170
規則管理作業 . . . 171
啓用及停用規則 . . . 172
編輯規則 . . . 172
複製規則 . . . 172
刪除規則 . . . 173
規則群組管理 . . . 173
檢視規則群組 . . . 173
建立群組 . . . 173
將項目指派給群組 . . . 174
編輯群組 . . . 174
將項目複製到其他群組 . . . 174
從群組中刪除項目 . . . 175
刪除群組 . . . 175
編輯建置區塊 . . . 175

規則頁面參數 176
規則頁面工具列 177
規則回應頁面參數 178

第 12 章 歷程關聯 187
歷程關聯概觀 187
建立歷程關聯設定檔 188
檢視歷程關聯執行的相關資訊 189

第 13 章 X-Force Threat Intelligence 資訊來源整合 191
X-Force Threat Intelligence 更新項目和伺服器 192
在 IBM Security QRadar 中啓用 X-Force 規則 192
加強型 X-Force Threat Intelligence 規則 192
使用 URL 分類建立規則以監視對特定類型網站的存取 193
在 X-Force Exchange 中尋找 IP 位址和 URL 資訊 194
管理誤判 195

第 14 章 報告管理 197
報告佈置 197
圖表類型 198
報告標籤工具列 199
圖形類型 200
建立自訂報告 201
編輯報告 204
檢視產生的報告 205
刪除產生的內容 205
手動產生報告 206
複製報告 206
共用報告 206
在報告上印品牌 207
報告群組 207
建立報告群組 208
編輯群組 208
共用報告群組 208
將報告指派給群組 210
將報告複製到其他群組 210
移除報告 210

聲明 211
商標 212
隱私權條款考量 213

名詞解釋 215
三劃 215
四劃 215
五劃 215
六劃 216
七劃 216
八劃 216
九劃 216
十劃 216
十一劃 217
十二劃 217
十三劃 218
十四劃 218
十七劃 219

十八劃. 219
十九劃. 219
A 219
C 219
D 219
F 219
H 220
I. 220
L 220
M 220
N 220
O 220
Q 220
R 220
S 220
T 220
W 221

索引 223

關於本手冊

《IBM® Security QRadar® SIEM 使用手冊》提供管理 IBM Security QRadar SIEM 的相關資訊，包括「儀表板」、「攻擊」、「日誌活動」、「網路活動」、「資產」及「報告」標籤。

目標讀者

本手冊面向負責調查及管理網路安全的所有 QRadar SIEM 使用者。 本手冊假定您具有 QRadar SIEM 存取權及公司網路和連網技術的知識。

技術文件

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 Accessing IBM Security Documentation Technical Note (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?uid=swg21616144)。

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、產品及服務係設計爲合法的全方位安全方法的一部分，因此必然將涉及其他作業程序，並且可能需要其他系統、產品或服務才能發揮最大效用。 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 7.2.6 版 中的使用者新增功能

IBM Security QRadar 7.2.6 版引入了最佳化檢索功能、比較內容的新 CRE 測試、授權改進等等。

可加速搜尋效能的最佳化索引

在舊版中，已針對每個 1 分鐘間隔建立索引。現在，使用 QRadar 7.2.6 版中的「超級索引」，會最佳化索引資料結構，並會在每個小時的結尾建立單一超級索引。尤其是在多小時搜尋時，現在 QRadar 會更佳地掃描索引，讓 Indicator of Compromise (IOC) 類型搜尋的效能增加達 10x。IP 位址、網域及主機名稱上的搜尋便是 IOC 類型搜尋的一些範例。QRadar 接收的所有新資料都會以新格式自動檢索。

只會最佳化接收的新資料的索引。如需改良歷程資料效能的相關資訊，請參閱 Optimizing your Ariel indexes in 7.2.6 technote (http://www.ibm.com/support/docview.wss?uid=swg21968002)。

新 CRE 測試

提供全新的自訂規則引擎 (CRE) 測試，可供用於比較一個內容與另一個內容，包括自訂內容。

您可以將來源 IP 位址與目的地 IP 位址相互比較。可根據自訂內容來比較使用者名稱。

進一步瞭解...

使用 AQL WHERE 子句文法在自訂規則引擎 (CRE) 中建置複雜的比較。可使用 AND/OR 邏輯、參照儲存器查閱與資產模型查詢。僅在建置 WHERE 子句時輸入條件。

進一步瞭解...

授權加強功能

QRadar 7.2.6 版可變更事件影響授權的方式。在舊版中，會針對您的授權計數 QRadar 產生的所有事件（例如 EPS 通知、系統通知及內部產生的日誌）。現在，不會針對您的授權計數下列內部事件：

- 系統通知
- 自訂規則引擎 (CRE)
- 審核
- ADE
- 資產側寫程式
- 所排程搜尋的結果
- 性能度量
- QRadar Risk Manager 問題、模擬及內部記載。

只有在客戶端的裝置上產生的事件才歸入您的授權。此外，使用遞送規則而捨棄之事件的 60% 也會歸回，最多爲每秒 2000 個事件 (EPS)。

檢視規則及搜尋結果中的參照集

現在，您對資料具備更多存取權。之前，如果您沒有管理者專用權，則無法使用參照集資訊。現在，管理者可授與您存取權，讓您能夠檢視搜尋結果及一般規則中的參照集。現在，您可以將參照集併入搜尋及一般規則中。您可以檢視參照集的清單、參照集的內容，並且可以匯出參照集。進一步瞭解...

右鍵功能表中的快速過濾器

右鍵功能表現在包含事件及流程的「快速過濾器」選項。使用「快速過濾器」準則在調查期間繪製資料圖表。您可以搜尋符合或不符合選擇的項目。新增符合/不符合過濾器之後，便可在右鍵功能表中使用更多的搜尋準則。進一步瞭解...

已改良查詢工作流程以便更快地存取資料

QRadar 可改良您與資料的互動方式，也可讓您快速展開攻擊發生之前及之後的時間。使用網路及日誌活動標籤上的時間序列圖表的選項，可快速變更顯示的時段，而不需要離開活動視圖。例如，如果您正在調查於星期二 4:30 PM 發生在端點上的攻擊，您可以從攻擊本身探查到事件。您可以查看在您查看之時間範圍之前或之後的幾分鐘內發生的事件，而無需開啓**編輯搜尋**頁面。您可以指定時段（精確到分鐘），或從下拉清單展開時段。進一步瞭解...

歷程關聯加強功能

IBM Security QRadar 7.2.6 版可讓您更好地瞭解威脅以及管理歷程關聯設定檔與結果：

增加了實際威脅的可見性

在 IBM Security QRadar 7.2.5 版中，已針對執行歷程關聯期間觸發的任何規則，建立歷程攻擊。在 7.2.6 版中，僅當觸發的規則指定必須針對偵測到的事件建立攻擊時，才會建立歷程攻擊。

改良的審核功能

每次執行或取消歷程關聯設定檔時都會建立審核記錄。這項變更提供了改良的監視功能並增加了可見性，讓您可以查看哪些使用者正在執行或取消歷程關聯執行。

新的攻擊搜尋功能

現在，您可以搜尋根據所選歷程關聯設定檔建立的攻擊。您也可以從已儲存的搜尋中排除歷程關聯結果。您可以使用這些新的搜尋參數，來區隔歷程關聯攻擊與用於報告的即時攻擊。

改良的歷程關聯設定檔管理

根據您正在處理的歷程資料量以及您指定的準則，您可能會發現需要一段時間才能完成關聯。現在，您可以取消正在執行或排入佇列等待執行的歷程關聯設定檔。

您可以在「歷程關聯」視窗中排序和過濾直欄，輕鬆找到您正在尋找的資訊。

當您檢視設定檔的執行歷程時，可以快速查看執行所建立的攻擊數目。在歷程關聯型錄上，只需要按一下就可以往下探查，以查看符合設定檔準則的事件或流程清單。

進一步瞭解...

新的 AQL 字串和統計功能

如果您要在正規表示式中尋找字串位置或取代字串，請在進階搜尋中使用下列 Ariel Query Language (AQL) 功能：

功能	說明
strpos	傳回字串在其他字串中的位置。
regex_replace	透過使用正規表示式作爲搜尋條件來取代字串。
first	傳回所指定直欄的前幾個實例。
last	傳回所指定直欄的後幾個實例。
stddev	傳回標準偏差範例。
stddevp	傳回標準偏差個體群。

如需相關資訊，請參閱 *IBM Security QRadar Ariel Query Language Guide* 中 Supported Functions 一節。

第 2 章 關於 QRadar SIEM

QRadar SIEM 是網路安全管理平台，可透過流程型網路知識、安全事件相關性及資產型漏洞評量的組合提供狀況提示及相符性支援。

預設授權金鑰

預設授權金鑰爲您提供五週的使用者介面存取權。 在您登入 QRadar SIEM 之後，視窗會顯示暫時授權金鑰到期的日期。如需安裝授權金鑰的相關資訊，請參閱 *IBM Security QRadar SIEM Administration Guide*。

安全異常狀況及憑證

如果使用的是 Mozilla Firefox Web 瀏覽器，您必須將異常狀況新增至 Mozilla Firefox 以登入 QRadar SIEM。如需相關資訊，請參閱 Mozilla Firefox Web 瀏覽器文件。

如果使用的是 Microsoft Internet Explorer Web 瀏覽器，在您存取 QRadar SIEM 系統時，畫面上會顯示網站安全憑證訊息。您必須選取**繼續此網站選項**，以登入 QRadar SIEM。

導覽 Web 型應用程式

在您使用 QRadar SIEM 時，使用 QRadar SIEM 使用者介面中可用的導覽選項，而非 Web 瀏覽器的**上一頁**按鈕。

安全智慧產品中的功能

IBM Security QRadar 產品說明文件說明所有 QRadar 產品中可能未提供的功能，例如攻擊、流程、資產及歷程關聯。根據您所使用的產品，您的部署中可能未提供部分記載的特性。請檢閱每個產品的功能以引導您至所需的資訊。

IBM Security QRadar SIEM 包含適用於內部部署的全範圍安全智慧功能。QRadar SIEM 會合併在整個網路配送的裝置端點與應用程式中的日誌來源事件資料，並對原始資料執行立即正規化和關聯活動，以區分實際威脅與誤判。

在代管環境中，使用 IBM Security Intelligence on Cloud 來收集、分析、保存及儲存大量網路與安全事件日誌。分析資料以便在開發威脅時提供可見性，並符合標準監視和報告需求，同時降低所有權總成本。

使用 IBM Security QRadar Log Manager 來收集、分析、保存及儲存大量網路與安全事件日誌。QRadar Log Manager 分析資料以便在開發威脅時提供可見性，它可協助您符合標準監視與報告需求。

尋求協助時，請使用下表，其中列出了產品的功能：

表 1. 比較 QRadar 功能

功能	QRadar SIEM	IBM Security Intelligence on Cloud	IBM Security QRadar Log Manager
支援代管部署	否	是	否
可自訂的儀表板	是	是	是
自訂規則引擎	是	是	是
管理網路和安全事件	是	是	是
管理主機和應用程式日誌	是	是	是
臨界值型警示	是	是	是
標準範本	是	是	是
資料保存	是	是	是
IBM Security X-Force® Threat Intelligence IP 信譽資訊來源整合	是	是	是
WinCollect 獨立式部署	是	是	是
WinCollect 受管理部署	是	否	是
QRadar Vulnerability Manager 整合	是	否	是
網路活動監視	是	否	否
資產側寫	是	是	否 [1]
攻擊管理	是	是	否
網路流程擷取和分析	是	否	否
歷程關聯	是	是	否
QRadar Risk Manager 整合	是	否	否
QRadar Incident Forensics 整合	是	否	否
[1] QRadar Log Manager 僅在安裝了 QRadar Vulnerability Manager 時追蹤資產資料。			

支援的 Web 瀏覽器

爲了 IBM Security QRadar 產品的功能正常運作，必須使用支援的 Web 瀏覽器。

存取 QRadar 系統時，會提示您輸入使用者名稱和密碼。 使用者名稱和密碼必須由管理者事先進行配置。

下列表格列出了支援的 Web 瀏覽器版本。

表 2. QRadar 產品支援的 Web 瀏覽器

Web 瀏覽器	支援的版本
Mozilla Firefox	38.0 延伸支援版
32 位元 Microsoft Internet Explorer（已啓用文件模式及瀏覽器模式）。	10.0
32 位元和 64 位元 Microsoft Internet Explorer（在文件模式下選取 Microsoft Internet Explorer 10）。	11.0

表 2. QRadar 產品支援的 Web 瀏覽器 (繼續)

Web 瀏覽器	支援的版本
Google Chrome	第 46 版

在 Internet Explorer 中啓用文件模式和瀏覽器模式

如果採用 Microsoft Internet Explorer 存取 IBM Security QRadar 產品，那麼必須啓用瀏覽器模式和文件模式。

程序

1. 在 Internet Explorer Web 瀏覽器中，按 F12 以開啓「開發者工具」視窗。
2. 按一下**瀏覽器模式**，並選取 Web 瀏覽器的版本。
3. 按一下**文件模式**，然後針對 Internet Explorer 版本選取 **Internet Explorer 標準**。

IBM Security QRadar 登入

IBM Security QRadar 是 Web 型應用程式。 QRadar 會將預設登入資訊用於 URL、使用者名稱及密碼。

在您登入 IBM Security QRadar 主控台時，使用下表中的資訊。

表 3. QRadar 的預設登入資訊

登入資訊	預設值
URL	https://<IP Address>，其中 <IP Address> 是 QRadar 主控台的 IP 位址。 若要在 IPv6 或混合環境中登入 QRadar，請以方括弧將 IP 位址括起： `https://[<IP Address>]`
使用者名稱	admin
密碼	在安裝過程中指派給 QRadar 的密碼。
授權金鑰	預設授權金鑰爲您提供 5 週的系統存取權。

RESTful API

使用表述性狀態轉移 (REST) 應用程式設計介面 (API) 來做出 HTTPS 查詢，並將 IBM Security QRadar 與其他解決方案整合。

存取權及使用者角色許可權

您在 QRadar 中必須具有管理使用者角色許可權才能存取和使用 RESTful API。 如需如何管理使用者角色許可權的相關資訊，請參閱*管理手冊*。

存取 REST API 技術文件使用者介面

API 使用者介面提供了下列 REST API 介面的說明和功能：

表 4. REST API 介面

REST API	說明
/api/ariel	查詢資料庫、搜尋、搜尋 ID，以及搜尋結果。
/api/asset_model	傳回模型中所有資產的清單。 您還可以列出所有可用的資產內容類型和已儲存的搜尋，並更新資產。
/api/auth	登出並使現行階段作業失效。
/api/help	返回 API 功能的清單。
/api/siem	傳回所有攻擊的清單。
/api/qvm	檢閱並管理 QRadar Vulnerability Manager 資料。
/api/reference_data	檢視並管理參照資料集合。
/api/qvm	擷取資產、漏洞、網路、開放的服務、網路和過濾器。 您還可以建立或更新補救通行證。
/api/scanner	檢視、建立或啓動與掃描設定檔相關的遠端掃描。

REST API 技術文件介面提供了一個架構，您可以使用它來收集將 QRadar 功能實作到其他產品中所需的必要程式碼。

1. 在 Web 瀏覽器中輸入下列 URL 以存取技術文件介面：https://*ConsoleIPaddress*/api_doc。
2. 按一下所要存取之 API 的標頭，例如，**/ariel**。
3. 按一下所要存取之端點的子標頭，例如， **/databases**。
4. 按一下 Experimental 或 Provisional 子標頭。

   註：

   API 端點標註爲 *experimental* 或 *stable*。

   Experimental
   指示 API 端點可能未經完全測試，可能在將來變更或移除，而不另行通知。

   Stable 指示 API 端點經過完全測試，且受支援。
5. 按一下**嘗試**以接收正確設定格式的 HTTPS 回應。
6. 檢閱並收集在協力廠商解決方案中實作所需的資訊。

QRadar API 討論區及程式碼範例

API 討論區提供了 REST API 的相關詳細資訊，其中包括對常見問題的回答以及可在測試環境中使用的帶標註的程式碼範例。 如需相關資訊，請參閱 API 討論區 (https://www.ibm.com/developerworks/community/forums/html/forum?id=b02461a3-9a70-4d73-94e8-c096abe263ca)。

使用者介面標籤

功能分爲數個標籤。 在您登入時，畫面上會顯示**儀表板**標籤。

您可以輕鬆地導覽標籤，以尋找您需要的資料或功能。

儀表板標籤

儀表板標籤是您登入時顯示的預設標籤。

儀表板標籤提供了支援多個儀表板的工作區環境，您可以藉以顯示網路安全、活動或 QRadar 所收集資料的視圖。 五個預設儀表板可用。 每個儀表板都包含可提供有關網路上所發生攻擊的摘要及詳細資訊之項目。 您也可以建立自訂儀表板，以讓您聚焦於安全或網路作業責任。 如需使用「儀表板」標籤的相關資訊，請參閱儀表板管理。

攻擊標籤

攻擊標籤將讓您檢視網路上發生的攻擊，您可以使用各種導覽選項或透過功能強大的搜尋來尋找。

透過**攻擊**標籤，您可以調查攻擊以判定問題的主要原因。 您也可以解決此問題。

如需**攻擊**標籤的相關資訊，請參閱攻擊管理。

日誌活動標籤

日誌活動標籤將讓您即時調查傳送至 QRadar 的事件日誌，執行功能強大的搜尋，以及使用可配置的時間序列圖表檢視日誌活動。

日誌活動標籤將讓您對事件資料執行深度調查。

如需相關資訊，請參閱日誌活動調查。

網路活動標籤

使用**網路活動**標籤即時調查傳送的流程，執行功能強大的搜尋，以及使用可配置的時間序列圖表檢視網路活動。

流程是兩個主機之間的通訊階段作業。 檢視流程資訊將讓您判定資料流量的通訊方式、通訊內容（如果已啓用內容擷取選項）及通訊者。 流程資料也包含通訊協定、ASN 值、IFIndex 值及優先順序等詳細資料。

如需相關資訊，請參閱網路活動調查。

資產標籤

QRadar 會自動探索網路上正在運作的資產、伺服器及主機。

自動探索基於被動流程資料及漏洞資料，容許 QRadar 建置資產設定檔。

資產設定檔提供網路中的每個已知資產的相關資訊，其中包括識別資訊（如果可用），以及每個資產上正在執行的服務。 此設定檔資料用來進行關聯，有助於減少誤判。

例如，某攻擊嘗試使用正在特定資產上執行的特定服務。 在此狀況中，QRadar 可以透過將攻擊與資產設定檔相關聯，來判定資產是否容易遭到此攻擊。 使用**資產**標籤，您可以檢視已瞭解的資產，或搜尋特定資產以檢視其設定檔。

如需相關資訊，請參閱資產管理。

報告標籤

報告標籤將讓您爲 QRadar 內的任何資料建立、配送及管理報告。

「報告」功能將讓您建立自訂的報告，以供作業及執行用途。 若要建立報告，您可以將資訊（如，安全或網路）結合成單一報告。 您也可以使用 QRadar 隨附的預先安裝的報告範本。

報告標籤也將讓您使用自訂的標誌在報告上印品牌。 此自訂作業對於將報告配送給不同的讀者是有益的。

如需報告的相關資訊，請參閱報告管理。

IBM Security QRadar Risk Manager

IBM Security QRadar Risk Manager 是個別安裝的軟體驅動裝置，用於監視裝置配置、模擬網路環境的變更，以及設定網路中風險和漏洞的優先順序。

IBM Security QRadar Risk Manager 使用配置資料從網路及安全裝置（如防火牆、路由器、交換器或 IPS、漏洞資訊來源及供應商安全來源）收集的資料。 此資料用於識別網路安全基礎架構內的安全、原則及相符性風險，以及這些風險被不當利用的概率。

註：如需 IBM Security QRadar Risk Manager 的相關資訊，請聯絡本地銷售代表。

管理標籤

管理者使用「管理」標籤來配置及管理使用者、系統、網路、外掛程式和元件。 具有管理專用權的使用者可以存取**管理**標籤。

表 1 說明了管理者可以在**管理**標籤中存取的管理工具。

表 5. QRadar 中可用的管理工具

管理工具	說明
系統配置	配置系統及使用者管理選項。
資料來源	配置日誌來源、流程來源及漏洞選項。
遠端網路及服務配置	配置遠端網路及服務群組。
部署編輯器	管理 QRadar 部署的個別元件。

您在**管理**標籤上進行的所有配置更新項目都會儲存至暫置區。完成所有變更後，可以在您的部署中，將配置更新項目部署至受管理主機。

QRadar 一般程序

QRadar 使用者介面上的各種控制項對於大部分使用者介面標籤是共用的。

下列小節說明了這些一般程序的相關資訊。

檢視訊息

訊息功能表位於使用者介面的右上角，提供對可用於讀取和管理系統通知之視窗的存取。

開始之前

若要在**訊息**視窗上顯示系統通知，管理者必須根據每一個通知訊息類型來建立規則，然後選取**自訂規則精靈**中的**通知**勾選框。

關於這項作業

訊息功能表指示您系統中未讀的系統通知數。 此指示器會增加數字，直到您關閉系統通知爲止。 對於每一個系統通知，**訊息**視窗會提供摘要，以及建立系統通知的日期戳記。您可以將滑鼠指標移至通知，以檢視更多明細。 您可以使用**訊息**視窗上的功能來管理系統通知。

系統通知也可以在**儀表板**標籤上獲取，在使用者介面的左下角可以顯示一個選用的蹦現視窗。 您在**訊息**視窗中執行的動作會延伸到**儀表板**標籤和蹦現視窗。 例如，如果您從**訊息**視窗關閉系統通知，則會從所有系統通知顯示畫面移除系統通知。

如需儀表板系統通知的相關資訊，請參閱系統通知項目。

訊息視窗提供下列功能：

表 6. 「訊息」視窗中可用的功能

功能	說明
全部	按一下**全部**，以檢視所有系統通知。 此選項是預設值，所以，僅當您選取了其他選項，並希望重新整理所有系統通知時才按**全部**。
性能	按一下**正常**，僅檢視具有嚴重性層次「正常」的系統通知。
錯誤	按一下**錯誤**，僅檢視具有嚴重性層次「錯誤」的系統通知。
警告	按一下**警告**，僅檢視具有嚴重性層次「警告」的系統通知。
資訊	按一下**參考**，僅檢視具有嚴重性層次「參考」的系統通知。
全部跳出	按一下**全部跳出**，以從系統關閉所有系統通知。 如果使用**正常**、**錯誤**、**警告**或**參考**圖示來過濾系統通知清單，則**檢視全部**圖示上的文字會變更爲下列其中一項： • **跳出所有錯誤** • **跳出所有性能** • **跳出所有警告** • **跳出所有警告** • **跳出所有參考資訊**

表 6. 「訊息」視窗中可用的功能 (繼續)

功能	說明
檢視全部	按一下**檢視全部**，以在**日誌活動**標籤中檢視系統通知事件。如果使用**正常**、**錯誤**、**警告**或**參考**圖示來過濾系統通知清單，則**檢視全部**圖示上的文字會變更爲下列其中一項： • **檢視所有錯誤** • **檢視所有性能** • **檢視所有警告** • **檢視所有參考資訊**
跳出	按一下系統通知旁的**跳出**圖示，以從您的系統關閉系統通知。

程序

1. 登入 QRadar。
2. 在使用者介面的右上角，按一下**訊息**。
3. 在**訊息**視窗上，檢視系統通知的詳細資料。
4. 選用項目。 若要細化系統通知清單，請按下列其中一項：
   - **錯誤**
   - **警告**
   - **資訊**
5. 選用項目。 若要關閉系統通知，請選擇下列選項：

選項	敘述
全部跳出	按一下關閉所有系統通知。
跳出	按一下要關閉之系統通知旁的**跳出**圖示。

6. 選用項目。 若要檢視系統通知的詳細資料，請將滑鼠指標移至該系統通知。

排序結果

您可以按一下直欄標題來排序表格中的結果。直欄頂端的箭頭指示排序的方向。

程序

1. 登入 QRadar。
2. 按一次直欄標頭，以降冪排列表格；按兩次以升冪排列表格。

重新整理與暫停使用者介面

您可以手動重新整理、暫停及播放標籤上顯示的資料。

關於這項作業

儀表板和**攻擊**標籤會每隔 60 秒自動重新整理一次。

如果您以「前次間隔（自動重新整理）」模式檢視**日誌活動**和**網路活動**標籤，則這些標籤會每隔 60 秒自動重新整理一次。

介面右上角的計時器會指示至自動重新整理標籤的時間量。

當您以「即時（串流）」或「前一分鐘（自動重新整理）」模式檢視**日誌活動**或**網路活動**標籤時，可以使用**暫停**圖示來暫停現行顯示畫面。

您還可以暫停**儀表板**標籤中的現行顯示畫面。 按一下儀表板項目內部的任何位置會自動暫停標籤。 計時器閃爍紅色，以指示現行顯示畫面暫停。

程序

1. 登入 QRadar。
2. 按一下您要檢視的標籤。
3. 選擇下列其中一個選項：

選項	敘述
重新整理	按一下標籤右上角的**重新整理**，以便重新整理標籤。
暫停	按一下以暫停標籤上的顯示畫面。
播放	按一下在暫停計時器之後重新啓動計時器。

調查 IP 位址

您可以使用數種方法來調查「儀表板」、「日誌活動」及「網路活動」標籤上 IP 位址的相關資訊。

程序

1. 登入 QRadar。
2. 按一下您要檢視的標籤。
3. 將您的滑鼠指標移至 IP 位址，以檢視 IP 位址的位置。
4. 用滑鼠右鍵按一下 IP 位址或資產名稱，並選取下列其中一項：

表 7. IP 位址資訊

選項	說明
導覽 > 依網路檢視	顯示與所選 IP 位址相關聯的網路。
導覽 > 依來源摘要檢視	顯示與所選來源 IP 位址相關聯的攻擊。
導覽 > 依目的地摘要檢視	顯示與所選目的地 IP 位址相關聯的攻擊。
資訊 > DNS 查閱	搜尋基於 IP 位址的 DNS 項目。
資訊 > WHOIS 查閱	搜尋遠端 IP 位址的登錄擁有者。 預設的 WHOIS 伺服器爲 whois.arin.net。
資訊 > 埠掃描	執行所選 IP 位址的「網路對映程式 (NMAP)」掃描。 僅當您的系統上已安裝 NMAP 時才能使用此選項。 如需安裝 NMAP 的相關資訊，請參閱您的供應商文件。

表 7. IP 位址資訊 (繼續)

選項	說明
資訊 > 資產設定檔	顯示資產設定檔資訊。 如果購買了 IBM Security QRadar Vulnerability Manager 並得到授權，則會顯示此選項。 如需相關資訊，請參閱*IBM Security QRadar Vulnerability Manager User Guide*。 如果 QRadar 透過掃描以主動方式，或透過流程來源以被動方式獲得設定檔資料，則可以使用此功能表選項。 如需相關資訊，請參閱*IBM Security QRadar SIEM Administration Guide*。
資訊 > 搜尋事件	搜尋與此 IP 位址相關聯的事件。
資訊 > 搜尋流程	搜尋與此 IP 位址相關聯的流程。
資訊 > 搜尋連線	搜尋與此 IP 位址相關聯的連線。 僅當您購買了 IBM Security QRadar Risk Manager，並連接了 QRadar 與 IBM Security QRadar Risk Manager 軟體驅動裝置時，才會顯示此選項。如需相關資訊，請參閱 *IBM Security QRadar Risk Manager User Guide*。
資訊 > 交換器埠查閱	確定 Cisco IOS 裝置上針對此 IP 位址的交換器埠。 此選項僅適用於使用**風險**標籤上的**探索裝置**選項探索的交換器。 **註**：此功能表選項在 QRadar Log Manager 中不可使用
資訊 > 視圖拓蹼	顯示**風險**標籤，它描述了您網路的 3 層拓蹼。僅當您購買了 IBM Security QRadar Risk Manager，並連接了 QRadar 與 IBM Security QRadar Risk Manager 軟體驅動裝置時，才能使用此選項。
執行漏洞掃描	選取**執行漏洞掃描**選項來於此 IP 位址上執行 IBM Security QRadar Vulnerability Manager 掃描。 僅當已購買 IBM Security QRadar Vulnerability Manager 並得到授權之後才會顯示此選項。 如需相關資訊，請參閱*IBM Security QRadar Vulnerability Manager User Guide*。

調查使用者名稱

您可以用滑鼠右鍵按一下使用者名稱，以存取更多功能表選項。使用這些選項來檢視使用者名稱或 IP 位址的相關資訊。

在購買 IBM Security QRadar Vulnerability Manager 及獲得其授權時，您才能調查使用者名稱。 如需相關資訊，請參閱 *IBM Security QRadar Vulnerability Manager User Guide*。

在您用滑鼠右鍵按一下使用者名稱時，可以選擇下列功能表選項。

表 8. 用於使用者名稱調查的功能表選項

選項	說明
檢視資產	顯示與所選取使用者名稱相關聯的現行資產。如需檢視資產的相關資訊，請參閱資產管理。
檢視使用者歷程	顯示過去 24 小時內與所選取使用者名稱相關聯的所有資產。
檢視事件	顯示與所選取使用者名稱相關聯的事件。 如需「事件清單」視窗的相關資訊，請參閱日誌活動監視。

如需自訂右鍵功能表的相關資訊，請參閱您產品的 *管理手冊*。

系統時間

QRadar 使用者介面的右角顯示系統時間，這是主控台上的時間。

主控台時間會同步化 QRadar 部署內的 QRadar 系統。主控台時間用於判定從其他裝置收到事件的時間，以取得正確的時間同步化關聯。

在分散式部署中，主控台可能與您的桌上型電腦中的時區不同。

在**日誌活動** 和**網路活動**標籤上套用時間型過濾器及搜尋時，您必須使用主控台系統時間來指定時間範圍。

套用時間型過濾器及在**日誌活動**標籤上搜尋時，您必須使用主控台系統時間來指定時間範圍。

更新使用者喜好設定

您可以設定 IBM Security QRadar SIEM 使用者介面中的使用者喜好設定，例如，語言環境。

程序

1. 若要存取您的使用者資訊，按一下**喜好設定**。
2. 更新喜好設定。

選項	敘述
使用者名稱	顯示您的使用者名稱。 您無法編輯這個欄位。
密碼	QRadar 使用者密碼儲存爲冗餘的 SHA-256 字串。 密碼必須符合下列準則： • 最少 6 個字元 • 最多 255 個字元 • 包含至少 1 個特殊字元 • 包含 1 個大寫字元
密碼（確認）	密碼確認

選項	敘述
電子郵件位址	電子郵件位址必須符合下列需求： • 最少 10 個字元 • 最多 255 個字元
語言環境	QRadar 提供下列語言：英文、簡體中文、繁體中文、日文、韓文、法文、德文、義大利文、西班牙文、俄文與葡萄牙文（巴西）。 如果您選擇不同的語言，則使用者介面以英文顯示。 使用其他關聯的文化慣例，例如，字元類型、對照、日期和時間格式，以及貨幣單位。
啓用蹦現通知	如果要啓用蹦現系統通知，以顯示在您的使用者介面上，請選取這個勾選框。

相關概念:

第 140 頁的『「快速過濾器」搜尋選項』
透過輸入使用簡式字詞或片語的文字搜尋字串來搜尋事件和流程有效負載。

存取線上說明

您可以透過主要 QRadar 使用者介面存取「QRadar 線上說明」。

若要存取「線上說明」，請按一下**說明 > 說明內容**。

調整直欄大小

您可以在 QRadar 中調整數個標籤上的直欄大小。

將滑鼠指標放在行上以區隔直欄，及將直欄邊緣拖曳至新位置。 您也可以調整直欄大小，方法是按兩下行以區隔直欄，來將直欄大小自動調整爲最大欄位的寬度。

註：標籤在串流模式下顯示記錄時，直欄調整大小無法在 Microsoft Internet Explorer 7.0 版 Web 瀏覽器中運作。

■面大小

具有管理專用權的使用者，可以配置 QRadar 中各種標籤上的表格中顯示的結果數上限。

第 3 章 儀表板管理

儀表板標籤是在登入時的預設視圖。

它提供了支援多個儀表板的工作區環境，您可以藉以顯示網路安全、活動或所收集資料的視圖。

儀表板可讓您將儀表板項目組織在功能視圖中，讓您聚焦於網路的特定區域。

使用「儀表板」標籤來監視安全事件行爲。

您可以自訂儀表板。 **儀表板**標籤上顯示的內容是使用者特定的。 在階段作業內進行的變更僅會影響您的系統。

預設儀表板

使用預設儀表板將項目自訂在功能視圖中。 這些功能視圖聚焦於網路的特定區域。

儀表板標籤提供五個預設儀表板，致力於安全、網路活動、應用程式活動、系統監視及相符性。

每個儀表板顯示屬於儀表板項目集的預設值。儀表板項目作爲導覽至更詳細資料的起點。 下表定義預設儀表板。

自訂儀表板

您可以自訂儀表板。 **儀表板**標籤上顯示的內容是使用者特定的。在 QRadar 階段作業內進行的變更僅會影響您的系統。

若要自訂**儀表板**標籤，您可以執行下列作業：

- 建立與您的責任相關的自訂儀表板。每位使用者最多 255 個儀表板；但是，如果您建立超過 10 個儀表板，可能會發生效能問題。
- 從預設或自訂儀表板新增及移除儀表板項目。
- 移動及定位項目以符合您的需求。 定位項目時，每個項目都會根據儀表板的比例自動調整大小。
- 新增基於任何資料的自訂儀表板項目。

例如，您可以新增儀表板項目，以提供代表前 10 個網路活動的時間序列圖形或長條圖。

若要建立自訂項目，您可以在**網路活動**或**日誌活動**標籤上建立已儲存的搜尋，然後選擇您希望在儀表板中呈現結果的方式。每個儀表板圖表都會顯示即時最新資料。 儀表板上的時間序列圖形每 5 分鐘重新整理一次。

自訂儀表板

您可以將數個儀表板項目新增至預設或自訂儀表板。

您可以自訂儀表板，來顯示及組織符合您的網路安全需求的儀表板項目。

有 5 個預設儀表板，您可以從**儀表板**標籤上的**顯示儀表板**清單框中存取它們。 如果您之前已檢視儀表板且已回到**儀表板**標籤，畫面上會顯示您檢視的最後一個儀表板。

流程搜尋

您可以透過**網路活動**標籤，顯示基於已儲存的搜尋準則的自訂儀表板項目。

新增項目 > **網路活動** > **流程搜尋**功能表中會列出流程搜尋項目。 流程搜尋項目的名稱與項目所基於的已儲存搜尋準則的名稱相符。

預設的已儲存的搜尋準則可用，且預先配置爲在**儀表板**標籤功能表上顯示流程搜尋項目。 您可以將更多流程搜尋儀表板項目新增至**儀表板**標籤功能表。 如需相關資訊，請參閱將搜尋型儀表板項目新增至新增項目清單。

在流程搜尋儀表板項目上，搜尋結果會在圖表上顯示即時最新資料。 支援的圖表類型爲時間序列、表格、圓餅圖及長條圖。 預設圖表類型爲長條圖。 這些圖表是可配置的。如需配置圖表的相關資訊，請參閱配置圖表。

時間序列圖表爲互動式。 使用時間序列圖表，您可以放大及瀏覽時間表來調查網路活動。

攻擊

您可以將數個與攻擊相關的項目新增至儀表板。

註：隱藏或關閉的攻擊不會包含在**儀表板**標籤中顯示的值中。 如需隱藏事件或已關閉事件的相關資訊，請參閱攻擊管理。

下表說明攻擊項目：

表 9. 攻擊項目

儀表板項目	說明
最近的攻擊	以長度列識別五個最近的攻擊，來通知您攻擊的重要性。指向攻擊名稱可檢視 IP 位址的詳細資訊。
最嚴重的攻擊	以長度列識別五個最嚴重的攻擊，來通知您攻擊的重要性。指向攻擊名稱可檢視 IP 位址的詳細資訊。
我的攻擊	**我的攻擊**項目顯示指派給您的 5 個最近攻擊。以長度列識別攻擊，來通知您攻擊的重要性。指向 IP 位址可檢視 IP 位址的詳細資訊。
前幾個來源	**前幾個來源**項目顯示前幾個攻擊來源。 以長度列識別每個來源，來通知您來源的重要性。 指向 IP 位址可檢視 IP 位址的詳細資訊。
前幾個本端目的地	**前幾個本端目的地**項目顯示前幾個本端目的地。 以長度列識別每個目的地，來通知您目的地的重要性。指向 IP 位址可檢視 IP 的詳細資訊
種類	**前幾個種類類型**項目顯示與攻擊最大數目相關聯的前 5 個種類。

日誌活動

日誌活動儀表板項目將容許您即時監視及調查事件。

註：隱藏或關閉的事件不會包含在**儀表板**標籤中顯示的值中。

表 10. 日誌活動項目

儀表板項目	說明
事件搜尋	您可以透過「日誌活動」標籤顯示基於已儲存搜尋準則的自訂儀表板項目。 在**新增項目 > 網路活動 > 事件搜尋**功能表中列出事件搜尋項目。 事件搜尋項目的名稱與項目所基於的已儲存搜尋準則名稱相符。 QRadar 包括預先配置爲在**儀表板**標籤功能表上顯示事件搜尋項目的預設已儲存搜尋準則。 您可以將更多事件搜尋儀表板項目新增至**儀表板**標籤功能表。 如需相關資訊，請參閱「將搜尋型儀表板項目新增至新增項目清單」。 在**日誌活動**儀表板項目上，搜尋結果會在圖表上顯示即時最新資料。支援的圖表類型爲時間序列、表格、圓餅圖及長條圖。 預設圖表類型爲長條圖。 這些圖表是可配置的。 時間序列圖表爲互動式。 您可以放大及瀏覽時間表來調查日誌活動。
依嚴重性列出的事件	**依嚴重性列出的事件**儀表板項目顯示依嚴重性分組的作用中事件數目。此項目將容許您查看依指派的嚴重性層次接收的事件數目。 嚴重性指出攻擊來源導致的威脅程度，與目的地應對攻擊的程度相關。 嚴重性範圍爲 0（低）至 10（高）。支援的圖表類型爲「表格」、「圓餅圖」及「長條圖」。
前幾個日誌來源	**前幾個日誌來源**儀表板項目顯示在前 5 分鐘內將事件傳送至 QRadar 的前 5 個日誌來源。 以圓餅圖指出從指定的日誌來源傳送的事件數。此項目將讓您檢視行爲中的潛在變更，例如，如果通常不在前 10 個清單中的防火牆日誌來源現在提供的內容佔整體訊息計數的大部分，您應調查此情況。支援的圖表類型爲「表格」、「圓餅圖」及「長條圖」。

最新報告

最新報告儀表板項目顯示前幾個最近產生的報告。

顯示畫面提供報告標題、產生報告的時間及日期，以及報告的格式。

系統摘要

系統摘要儀表板項目提供過去 24 小時內活動的高階摘要。

在摘要項目內，您可以檢視下列資訊：

- **每秒的現行流程數** - 顯示每秒的流程比率。
- **流程數（過去 24 小時）** - 顯示過去 24 小時內顯示的作用中流程總數。
- **每秒的現行事件數** - 顯示每秒的事件比率。
- **新事件數（過去 24 小時）** - 顯示過去 24 小時內收到的新事件總數。
- **更新的攻擊數（過去 24 小時）** - 顯示過去 24 小時內已使用新證明建立或修改的攻擊總數。
- **資料縮減比例** - 顯示基於過去 24 小時內偵測到的事件總數與過去 24 小時內修改的攻擊數目的資料縮減比例。

風險監視儀表板

您可以使用**風險監視**儀表板來監視資產、原則和原則群組的原則風險及原則風險變更。

依預設，**風險監視**儀表板顯示**風險**和**風險變更項目**，它們監視「高漏洞」、「中漏洞」和「低漏洞」原則群組中資產的原則風險分數，以及 CIS 原則群組中原則風險分數的合規性通過率及歷程變更。

除非 IBM Security QRadar Risk Manager 已獲授權，否則「風險監視」儀表板項目不會顯示出來。如需相關資訊，請參閱《QRadar Risk Manager 使用手冊》。

若要檢視預設**風險監視**儀表板，請在**儀表板**標籤上選取**顯示儀表板 > 風險監視**。

相關工作:

『監視原則合規性』
建立儀表板項目，用於顯示所選資產、原則和原則群組的原則合規性通過率和原則風險評分。

第 22 頁的『監視風險變更』
建立儀表板項目，用於顯示所選資產、原則和原則群組的每日、每週和每月原則風險變更。

監視原則合規性

建立儀表板項目，用於顯示所選資產、原則和原則群組的原則合規性通過率和原則風險評分。

程序

1. 按一下**儀表板**標籤。
2. 在工具列上，按一下**新建儀表板**。
3. 輸入原則合規性儀表板的名稱和說明。
4. 按一下**確定**。
5. 在工具列上，選取**新增項目 > 風險管理程式 > 風險**。

   僅當 IBM Security QRadar Risk Manager 已獲授權時，**風險管理程式**儀表板項目才會顯示出來。

6. 在您新的儀表板項目的標頭上，按一下**設定**圖示。
7. 使用**圖表類型**、**顯示前幾個**和**排序**清單來配置圖表。
8. 從**群組**清單中，選取要監視的群組。 如需相關資訊，請參閱表格中的步驟 9。

   當您選取**資產**選項時，會在**風險**儀表板項目底端出現**風險 > 原則管理 > 依資產**頁面的鏈結。 **依資產**頁面顯示根據所選**原則群組**返回的全部結果的更多詳細資訊。如需特定資產的相關資訊，請從**圖表類型**清單中選取**表格**，然後按一下**資產**直欄中的鏈結，以在**依資產**頁面中檢視資產的詳細資料。

   當您選取**原則**選項時，會在**風險**儀表板項目底端出現**風險 > 原則管理 > 依原則**頁面的鏈結。 **依原則**頁面顯示根據所選**原則群組**返回的全部結果的更多詳細資訊。如需特定原則的相關資訊，請從**圖表類型**清單中選取**表格**，然後按一下**原則**直欄中的鏈結，以在**依原則**頁面中檢視原則的詳細資料。
9. 從**圖形**清單中，選取要使用的圖形類型。 如需相關資訊，請參閱下表：

群組	資產通過百分比	原則檢查通過百分比	原則群組通過百分比	原則風險評分
全部	傳回資產、原則和原則群組之間平均資產百分比通過率。	傳回資產、原則和原則群組之間的平均原則檢查百分比通過率。	傳回所有資產、原則和原則群組之間的平均原則群組通過率。	傳回所有資產、原則和原則群組之間的平均風險評分。
資產	傳回資產是否通過資產合規性（100%=通過，0%=未通過）。 使用此設定來顯示哪些資產與原則群組通過合規性相關聯。	傳回資產通過的原則檢查百分比。 使用此設定來顯示對於與原則群組相關聯的每個資產，通過資產檢查的百分比。	傳回與通過合規性的資產相關聯的原則子群組百分比。	傳回與每一個資產相關聯的原則問題的所有重要性因子值之和。 使用此設定來檢視對於與所選原則群組相關聯的每個資產的原則風險。
原則	傳回與原則群組中通過合規性的每一個原則相關聯的所有資產。 使用此設定來監視與原則群組中的每一個原則相關聯的所有資產是通過還是未通過合規性。	傳回原則群組中每個原則的通過原則檢查百分比。 使用此設定來監視每個原則有多少原則檢查未通過。	傳回原則的通過合規性部分的原則子群組的百分比。	傳回原則群組中每一個原則問題的重要性因子值之。 使用此設定來檢視原則群組中每一個原則的重要性因子。
原則群組	傳回通過所選原則群組整體的合規性的資產百分比。	傳回通過所選原則群組整體的每個原則的原則檢查百分比。	傳回原則群組內通過合規性之原則子群組的百分比。	傳回原則群組中所有原則問題的所有重要性因子值之和。

10. 從**原則群組**清單中，選取要監視的原則群組。
11. 按一下**儲存**。

監視風險變更

建立儀表板項目，用於顯示所選資產、原則和原則群組的每日、每週和每月原則風險變更。

關於這項作業

使用此儀表板來比較一段時間內原則群組的「原則風險評分」、「原則檢查」和「原則」值的變更。

風險變更儀表板項目使用箭頭來指出在所選擇的時段內，提高、降低或保持不變的所選值的原則風險位於何處。

- 紅色箭頭下方的數字指出顯示風險提高的值。
- 灰色箭頭下方的數字指出風險無變化的值。
- 綠色箭頭下方的數字指出顯示風險降低的值。

程序

1. 按一下**儀表板**標籤。
2. 在工具列上，按一下**新建儀表板**。
3. 輸入原則合規性儀表板的名稱和說明。
4. 按一下**確定**。
5. 在工具列上，選取**新增項目 > 風險管理程式 > 風險變更**。

   僅當 IBM Security QRadar Risk Manager 已獲授權時，**風險管理程式**儀表板項目才會顯示出來。
6. 在您新的儀表板項目的標頭上，按一下**設定**圖示。
7. 從**原則群組**清單中，選取要監視的原則群組。
8. 從**要比較的值**清單中選取選項：
   - 如果您要查看所選原則群組中所有原則問題的重要性因素的累積變更，請選取**原則風險評分**。
   - 如果您要查看所選原則群組中有多少原則檢查已變更，請選取**原則檢查**。
   - 如果您要查看所選原則群組中有多少原則已變更，請選取**原則**。
9. 從**變化時間**清單中選取要監視的風險變更時段：
   - 如果您要將來自今日上午 12:00 的風險變更與昨日的風險變更進行比較，請選取**日**。
   - 如果您要將來自本週星期一上午 12:00 的風險變更與上週的風險變更進行比較，請選取**週**。
   - 如果您要將來自本月第一日上午 12:00 的風險變更與上個月的風險變更進行比較，請選取**月**。
10. 按一下**儲存**。

漏洞管理項目

在購買 IBM Security QRadar Vulnerability Manager 及獲得其授權時，才會顯示「漏洞管理」儀表板項目。

如需相關資訊，請參閱 *IBM Security QRadar Vulnerability Manager User Guide*。

您可以透過**漏洞**標籤顯示基於已儲存搜尋準則的自訂儀表板項目。在**新增項目 > 漏洞管理 > 漏洞搜尋**功能表中列出搜尋項目。 搜尋項目的名稱與項目所基於的已儲存搜尋準則名稱相符。

QRadar 包括預先配置爲在**儀表板**標籤功能表上顯示搜尋項目的預設已儲存搜尋準則。 您可以將更多搜尋儀表板項目新增至**儀表板**標籤功能表。

支援的圖表類型爲表格、圓餅圖及長條圖。 預設圖表類型爲長條圖。 這些圖表是可配置的。

系統通知

「系統通知」儀表板項目顯示系統收到的事件通知。

爲使通知顯示在**系統通知**儀表板項目中，管理者必須建立基於每個通知訊息類型的規則，然後選取「自訂規則精靈」中的**通知**勾選框。

如需如何配置事件通知及建立事件規則的相關資訊，請參閱 *IBM Security QRadar SIEM Administration Guide*。

在**系統通知**儀表板項目上，您可以檢視下列資訊：

- **旗標** - 顯示指出通知嚴重性層次的符號。 指向此符號，可檢視嚴重性層次的相關詳細資料。
  - **性能**圖示
  - **資訊**圖示 (?)
  - **錯誤**圖示 (X)
  - **警告** 圖示 (!)
- **建立時間** - 顯示自建立通知以來經歷的時間量。
- **說明** - 顯示通知的相關資訊。
- **跳出圖示 (x)** - 將讓您關閉系統通知。

您可以將滑鼠移在通知上，以檢視相關詳細資料：

- **主機 IP** - 顯示已產生通知的主機的主機 IP 位址。
- **嚴重性** - 顯示已建立此通知的發生事件的嚴重性層次。
- **低階種類** - 顯示與已產生此通知的發生事件相關聯的低階種類。 例如：服務中斷。
- **有效負載** - 顯示與已產生此通知的發生事件相關聯的有效負載內容。
- **建立時間** - 顯示自建立通知以來經歷的時間量。

在您新增**系統通知**儀表板項目時，系統通知也可能會在 QRadar 使用者介面中顯示爲蹦現通知。 這些蹦現通知顯示在使用者介面的右下角，而不管選取的標籤。

蹦現通知僅適用於具有管理許可權的使用者，且依預設已啓用。 若要停用蹦現通知，請選取**使用者喜好設定**，並清除**啓用蹦現通知**勾選框。

在「系統通知」蹦現視窗中，會強調顯示佇列中的通知數目。 例如，如果標頭中顯示 (1-12)，則現行通知爲將顯示的 1 個（共 12 個）通知。

「系統通知」蹦現視窗將提供下列選項：

- **下一個圖示 (>)** - 顯示下一個通知訊息。 例如，如果現行通知訊息爲第 3 個（共 6 個），請按一下圖示以檢視第 4 個（共 6 個）。
- **關閉圖示 (X)** - 關閉此通知蹦現視窗。
- （**詳細資料**） - 顯示此系統通知的相關資訊。

網際網路威脅資訊中心

「網際網路威脅資訊中心」儀表板項目是內嵌的 RSS 資訊來源，可爲您提供有關安全問題、每日威脅評量、安全新聞及威脅儲存庫的最新諮詢。

「現行威脅層次」圖指出現行威脅層次，並提供 IBM Internet Security Systems 網站的「現行網際網路威脅層次」頁面的鏈結。

儀表板項目中列出了現行諮詢。 若要檢視諮詢的摘要，請按一下諮詢旁邊的**箭頭**圖示。諮詢會展開以顯示摘要。 再次按一下**箭頭**圖示可隱藏摘要。

若要調查完整諮詢，請按一下相關聯的鏈結。 IBM Internet Security Systems 網站會在另一個瀏覽器視窗中開啓，及顯示完整諮詢詳細資料。

建立自訂儀表板

您可以建立自訂儀表板，來檢視符合特定需求的儀表板項目群組。

關於這項作業

在您建立自訂儀表板之後，新的儀表板會顯示在**儀表板**標籤中，且會列在**顯示儀表板**清單框中。 依預設，新的自訂儀表板是空的；因此，您必須將項目新增至儀表板。

程序

1. 按一下**儀表板**標籤。
2. 按一下**新建儀表板**圖示。
3. 在**名稱**欄位中，鍵入儀表板的唯一名稱。 長度上限爲 65 個字元。
4. 在**說明**欄位中，鍵入儀表板的說明。 長度上限爲 255 個字元。此說明顯示在**顯示儀表板**清單框中的儀表板名稱的工具提示中。
5. 按一下**確定**。

使用儀表板來調查日誌或網路活動

基於搜尋的儀表板項目會提供**日誌活動**或**網路活動**標籤的鏈結，容許您進一步調查日誌或網路活動。

關於這項作業

若要從**日誌活動**儀表板項目調查流程：

1. 按一下**檢視日誌活動**鏈結。 此時會出現**日誌活動**標籤，顯示符合您儀表板項目之參數的結果與兩張圖表。

若要從**網路活動**儀表板項目調查流程：

1. 按一下**檢視網路活動**鏈結。此時會出現「網路活動」標籤，顯示符合您儀表板項目之參數的結果與兩張圖表。

此時會出現**網路活動**標籤，顯示符合您儀表板項目之參數的結果與兩張圖表。 **日誌活動**或**網路活動**標籤上顯示的圖表類型視儀表板項目中配置的圖表而定：

圖表類型	說明
長條圖、圓餅圖與表格	**日誌活動**或**網路活動**標籤顯示流程詳細資料的長條圖、圓餅圖與表格。
時間序列	**日誌活動**或**網路活動**標籤根據下列準則來顯示圖表： 1. 如果時間範圍小於或等於 1 小時，則顯示事件或流程詳細資料的時間序列圖表、長條圖與表格。 2. 如果時間範圍超過 1 小時，則顯示時間序列圖表，並提示您按一下「更新詳細資料」。 此動作會啓動移入事件或流程詳細資料的搜尋，並產生長條圖。 當搜尋完成後，會顯示事件或流程詳細資料的長條圖與表格。

配置圖表

您可以配置**日誌活動**、**網路活動**及**連線**，如果適用，儀表板項目會指定圖表類型及您要檢視的資料物件數量。

關於這項作業

表 11. 配置圖表. 參數選項

選項	說明
要圖形化的值	從清單框中，選取您要在圖表上圖形化的物件類型。 選項包括搜尋參數中包含的所有正規化及自訂事件或流程參數。
圖表類型	從清單框中，選取您要檢視的圖表類型。 選項包括： 1. **長條圖** - 以長條圖顯示資料。此選項僅適用於分組事件或流程。 2. **圓餅圖** - 以圓餅圖顯示資料。此選項僅適用於分組事件或流程。 3. **表格** - 以表格顯示資料。 此選項僅適用於分組事件或流程。 4. **時間序列** - 顯示互動式折線圖，來代表符合指定時間間隔的記錄。
顯示前幾個	從清單框中，選取您要在圖表中檢視的物件數目。 選項包括 **5** 及 **10**。 預設值爲 **10**。
擷取時間序列資料	選取此勾選框可啓用時間序列擷取。 在您選取此勾選框時，圖表功能會開始累計時間序列圖表的資料。 依預設，此選項已停用。
時間範圍	從清單框中，選取您要檢視的時間範圍。

您的自訂圖表配置會保留，因此每次您存取**儀表板**標籤時，它們會顯示爲已配置。

會累計資料，從而在您執行時間序列儲存的搜尋時，具有可用事件或流程資料的快取來顯示先前時段的資料。累計參數由**要圖形化的值**清單框中的星號 (*) 表示。 如果您選取未累計（無星號）的要圖形化的值，時間序列資料將無法使用。

程序

1. 按一下**儀表板**標籤。
2. 從**顯示儀表板**清單框中，選取包含您要自訂的項目的儀表板。
3. 在您要配置的儀表板項目的標頭上，按一下**設定**圖示。
4. 配置圖表參數。

移除儀表板項目

您可以隨時從儀表板移除項目和重新新增項目。

關於這項作業

當您從儀表板移除項目時，不會完全移除項目。

程序

1. 按一下**儀表板**標籤。
2. 從**顯示儀表板**清單框中，選取要從其移除項目的儀表板。
3. 在儀表板項目標頭上，按一下紅色的 [x] 圖示，以從儀表板移除項目。

分離儀表板項目

您可以從儀表板分離項目，及將項目顯示在桌面系統上的新視窗中。

關於這項作業

在您分離儀表板項目時，雖然原始儀表板項目會保留在**儀表板**標籤上，但具有重複儀表板項目的分離視窗仍然會開啓，且在排定的間隔重新整理。 如果您關閉 QRadar 應用程式，分離的視窗仍然會開啓以進行監視，且會繼續重新整理，直到您手動關閉視窗或關閉您的電腦系統。

程序

1. 按一下**儀表板**標籤。
2. 從**顯示儀表板**清單框中，選取您要分離項目的儀表板。
3. 在儀表板項目標頭上，按一下綠色圖示以分離儀表板項目，然後在個別視窗中開啓此項目。

重新命名儀表板

您可以重新命名儀表板及更新說明。

程序

1. 按一下**儀表板**標籤。
2. 從**顯示儀表板**清單框中，選取要編輯的儀表板。

3. 在工具列上，按一下**重新命名儀表板**圖示。
4. 在**名稱**欄位中，鍵入儀表板的新名稱。 最大長度爲 65 個字元。
5. 在**說明**欄位中，鍵入儀表板的新說明。 最大長度爲 255 個字元。
6. 按一下**確定**。

刪除儀表板

您可以刪除儀表板。

關於這項作業

在您刪除儀表板之後，**儀表板**標籤會重新整理，且畫面上會顯示在**顯示儀表板**清單框中列出的第一個儀表板。 您刪除的儀表板不再顯示在**顯示儀表板**清單框中。

程序

1. 按一下**儀表板**標籤。
2. 從**顯示儀表板**清單框中，選取您要刪除的儀表板。
3. 在工具列上，按一下**刪除儀表板**。
4. 按一下**是**。

管理系統通知

您可以指定要在**系統通知**儀表板上顯示的通知數，並在讀取系統通知之後將其關閉。

開始之前

請確保**系統通知**儀表板項目新增至您的儀表板。

程序

1. 在「系統通知」儀表板項目標頭上，按一下**設定**圖示。
2. 從**顯示**清單框中，選取要檢視的系統通知數。
   - 選項爲 **5**、**10**（預設值）、**20**、**50** 與**全部**。
   - 若要檢視過去 24 小時內登入的所有系統通知，請按一下**全部**。
3. 若要關閉系統通知，請按一下**刪除**圖示。

將搜尋型儀表板項目新增至新增項目清單

您可以將搜尋型儀表板項目新增至**新增項目**功能表。

開始之前

若要將事件及流程搜尋儀表板項目新增至**儀表板**標籤上的**新增項目**功能表，您必須存取**日誌活動**或**網路活動**標籤來建立搜尋準則，以指定搜尋結果可以顯示在**儀表板**標籤上。搜尋準則還必須指定根據參數分組結果。

程序

1. 選擇：
   - 若要新增流程搜尋儀表板項目，請按一下**網路活動**標籤。

- 若要新增事件搜尋儀表板項目，請按一下**日誌活動**標籤。

2. 從**搜尋**清單框中，選擇下列其中一個選項：
   - 若要建立搜尋，請選取**新建搜尋**。
   - 若要編輯已儲存的搜尋，請選取**編輯搜尋**。
3. 根據需要配置或編輯搜尋參數。
   - 在「編輯搜尋」窗格上，選取**包含在我的儀表板中**選項。
   - 在「直欄定義」窗格上，選取直欄，然後按一下**新增直欄**圖示以將直欄移至**分組依據**清單。
4. 按一下**過濾器**。 畫面上會顯示搜尋結果。
5. 按一下**儲存準則**。 請參閱「將搜尋準則儲存在攻擊標籤上」
6. 按一下**確定**。
7. 驗證已儲存的搜尋準則已順利將事件或流程搜尋儀表板項目新增至**新增項目**清單
   a. 按一下**儀表板**標籤。
   b. 選擇下列其中一個選項：
   a. 若要驗證事件搜尋項目，請選取**新增項目 > 日誌活動 > 事件搜尋 > 新增項目**。
   b. 若要驗證流程搜尋項目，請選取**新增項目 > 網路活動 > 流程搜尋**。 儀表板項目會顯示在清單上，名稱與已儲存的搜尋準則相同。

第 4 章 攻擊管理

您可以將事件及流程與在相同攻擊中多個網路間的目的地 IP 位址相關聯。您可以有效地調查網路中的每個攻擊。

限制： 您無法在 IBM Security QRadar Log Manager 中管理攻擊。如需 IBM Security QRadar SIEM 與 IBM Security QRadar Log Manager 之間差異的相關資訊，請參閱第 5 頁的『安全智慧產品中的功能』。

您可以導覽**攻擊**標籤的各種頁面來調查事件及流程詳細資料，以判定已導致攻擊的唯一事件及流程。

攻擊概觀

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

您也可以搜尋基於各種準則的攻擊。 如需搜尋攻擊的相關資訊，請參閱第 142 頁的『攻擊搜尋』。

攻擊許可權考量

所有使用者都可以檢視所有攻擊，而不管哪個日誌來源或流程來源與攻擊相關聯。

攻擊標籤不使用裝置層次使用者許可權來判定每位使用者可以檢視的攻擊；而是由網路許可權判定。

如需裝置層次許可權的相關資訊，請參閱 *IBM Security QRadar SIEM Administration Guide*。

重要詞彙

使用**攻擊**標籤，您可以存取及分析「攻擊」、「來源 IP 位址」及「目的地 IP 位址」。

項目	說明
攻擊	攻擊包括源於某個來源（如主機或日誌來源）的多個事件或流程。**攻擊**標籤顯示攻擊，其中包括可對攻擊長度進行協同作業及驗證的資料流量和漏洞。 每次重新評估攻擊時，會由對攻擊執行的數項測試來判定攻擊的長度。 當事件新增至攻擊時，會以排定的間隔進行重新評估。
來源 IP 位址	來源 IP 位址指定嘗試侵害網路上元件安全的裝置。來源 IP 位址可以使用各種攻擊方法（如勘察或「阻斷服務 (DoS)」攻擊）以嘗試進行未獲授權存取。
目的地 IP 位址	目的地 IP 位址指定來源 IP 位址嘗試存取的網路裝置。

攻擊保留

在**管理**標籤上，您可以配置攻擊保留期系統設定，以在配置的時段之後從資料庫移除攻擊。

預設攻擊保留期爲三天。 您必須具有管理許可權，才能存取**管理**標籤及配置系統設定。配置臨界值時，任何定義的臨界值爲五天。

關閉攻擊時，關閉的攻擊會在攻擊保留期過後從資料庫中移除。 如果攻擊發生更多事件，會建立新的攻擊。 如果您執行包含關閉的攻擊的搜尋，搜尋結果中會顯示此項目（如果它尚未從資料庫中移除）。

攻擊監視

使用**攻擊**標籤上可用的不同視圖，您可以監視攻擊以判定目前網路上發生的攻擊。

系統會先從最長的長度開始，列出攻擊。 您可以尋找及檢視特定攻擊的詳細資料，然後在需要時對攻擊執行動作。

在您透過各種視圖開始導覽之後，標籤頂端會顯示現行視圖的導覽軌跡。 如果您要回到之前檢視的頁面，請按一下導覽軌跡上的頁面名稱。

從**攻擊**標籤上的導覽功能表中，您可以存取下面表格中列出的下列頁面。

*表 12. 可以從**攻擊**標籤存取的頁面*

頁面	說明
我的攻擊	顯示指派給您的所有攻擊。
所有攻擊	顯示網路上的所有廣域攻擊。
依種類	顯示依高階及低階種類分組的所有攻擊。
依來源 IP	顯示依攻擊中涉及的來源 IP 位址分組的所有攻擊。
依目的地 IP	顯示依攻擊中涉及的目的地 IP 位址分組的所有攻擊。
依網路	顯示依攻擊中涉及的網路分組的所有攻擊。
規則	可讓您存取「規則」頁面，您可以從中檢視及建立自訂規則。只有在您具有「檢視自訂規則」角色許可權時，才顯示此選項。如需相關資訊，請參閱規則管理。

監視「所有攻擊」或「我的攻擊」頁面

您可以在「所有攻擊」或「我的攻擊」頁面上監視攻擊。

開始之前

「所有攻擊」頁面顯示在您的網路中發生的所有攻擊清單。 「我的攻擊」頁面顯示指派給您的攻擊清單。

關於這項作業

此表格頂端顯示套用到搜尋結果的攻擊搜尋參數的詳細資料（若有）。 若要清除這些搜尋參數，可以按一下**清除過濾器**。如需搜尋攻擊的相關資訊，請參閱攻擊搜尋。

註：若要更詳細檢視摘要頁面上的窗格，請按一下相關聯的工具列選項。 例如，如果要檢視來源 IP 位址的詳細資料，請按一下**來源**。 如需工具列選項的相關資訊，請參閱攻擊標籤工具列功能。

程序

1. 按一下**攻擊**標籤。
2. 在導覽功能表上，選取**所有攻擊**或**我的攻擊**。
3. 您可以利用下列選項來精進攻擊清單：
   - 從**檢視攻擊**清單框中，選取選項以過濾特定時間範圍的攻擊清單。
   - 按一下**現行搜尋參數**窗格中顯示的各個過濾器旁邊的**清除過濾器**鏈結。
4. 按兩下您要檢視的攻擊。
5. 在「攻擊摘要」頁面上，檢查攻擊的詳細資料。 請參閱攻擊參數。
6. 對攻擊執行所有必要的動作。

監視依種類分組的攻擊

您可以在「依種類詳細資料」頁面上監視攻擊，該頁面提供在高階種類上群組的攻擊清單。

關於這項作業

事件計數、**流程計數**和**來源計數**之類的計數欄位不考量使用者的網路許可權。

程序

1. 按一下**攻擊**標籤。
2. 在導覽功能表上，按一下**依種類**。
3. 若要檢視特定高階種類的低階種類群組，請按一下高階種類名稱旁的箭頭圖示。
4. 若要檢視低階種類的攻擊清單，請按兩下低階種類。
5. 按兩下您要檢視的攻擊。
6. 在「攻擊摘要」頁面上，檢查攻擊的詳細資料。 請參閱攻擊參數。
7. 對攻擊執行所有必要的動作。 請參閱攻擊管理作業。

監視依來源 IP 分組的攻擊

在「來源」頁面上，您可以監視依來源 IP 位址分組的攻擊。

關於這項作業

來源 IP 位址指定因爲對於您系統的攻擊而產生攻擊的主機。 系統會先從長度最高的 IP 位址開始，列出所有的來源 IP 位址。 攻擊清單僅顯示具有作用中的攻擊的來源 IP 位址。

程序

1. 按一下**攻擊**標籤。
2. 按一下**依來源 IP**。
3. 您可以使用下列選項來精進攻擊清單：
   - 從**檢視攻擊**清單框中，選取選項以過濾特定時間範圍的攻擊清單。
   - 按一下**現行搜尋參數**窗格中顯示的各個過濾器旁邊的**清除過濾器**鏈結。
4. 按兩下您要檢視的群組。
5. 若要檢視來源 IP 位址的本端目的地 IP 位址清單，請按一下「來源」頁面工具列上的**目的地**。
6. 若要檢視與此來源 IP 位址相關聯的攻擊清單，請按一下「來源」頁面工具列上的**攻擊**。
7. 按兩下您要檢視的攻擊。
8. 在「攻擊摘要」頁面上，檢查攻擊的詳細資料。 請參閱攻擊參數。
9. 對攻擊執行所有必要的動作。 請參閱攻擊管理作業。

監視依目的地 IP 分組的攻擊

在「目的地」頁面上，您可以監視依本端目的地 IP 位址分組的攻擊。

關於這項作業

系統會先從長度最高的 IP 位址開始，列出所有的目的地 IP 位址。

程序

1. 按一下**攻擊**標籤。
2. 按一下**依目的地 IP**。
3. 您可以使用下列選項來精進攻擊清單：
   - 從**檢視攻擊**清單框中，選取選項以過濾特定時間範圍的攻擊清單。
   - 按一下**現行搜尋參數**窗格中顯示的各個過濾器旁邊的**清除過濾器**鏈結。
4. 按兩下您要檢視的目的地 IP 位址。
5. 若要檢視與此目的地 IP 位址相關聯的攻擊清單，請按一下「目的地」頁面工具列上的**攻擊**。
6. 若要檢視與此目的地 IP 位址相關聯的來源 IP 位址清單，請按一下「目的地」頁面工具列上的**來源**。
7. 按兩下您要檢視的攻擊。
8. 在「攻擊摘要」頁面上，檢查攻擊的詳細資料。 請參閱攻擊參數。
9. 對攻擊執行所有必要的動作。 請參閱攻擊管理作業。

監視依網路分組的攻擊

在網路頁面上，您可以監視依網路分組的攻擊。

關於這項作業

系統會先從長度最高的網路開始，列出所有的網路。

程序

1. 按一下**攻擊**標籤。
2. 在導覽功能表上，按一下**依網路**。
3. 按兩下您要檢視的網路。
4. 若要檢視與此網路相關聯的來源 IP 位址清單，請按一下「網路」頁面工具列上的**來源**。
5. 若要檢視與此網路相關聯的目的地 IP 位址清單，請按一下「網路」頁面工具列上的**目的地**。
6. 若要檢視與此網路相關聯的攻擊清單，請按一下「網路」頁面工具列上的**攻擊**。
7. 按兩下您要檢視的攻擊。
8. 在「攻擊摘要」頁面上，檢查攻擊的詳細資料。 請參閱攻擊參數。
9. 對攻擊執行所有必要的動作。 請參閱攻擊管理作業。

攻擊管理作業

在監視攻擊時，您可以對攻擊執行動作。

您可以執行下列動作：

- 新增附註
- 移除攻擊
- 保護攻擊
- 將攻擊資料匯出至 XML 或 CSV
- 將攻擊指派給其他使用者
- 傳送電子郵件通知
- 將攻擊標示爲追蹤
- 從任何攻擊清單隱藏或關閉攻擊

若要對多個攻擊執行動作，請在您選取所要的每個攻擊時按住 Ctrl 鍵。若要檢視新頁面上的攻擊詳細資料，請在按兩下攻擊時按住 Ctrl 鍵。

新增附註

您可以將附註新增至**攻擊**標籤上的任何攻擊。 「附註」可以包含您要爲攻擊擷取的資訊，如「客戶支援中心」通行證號碼或攻擊管理資訊。

關於這項作業

附註可以包含多達 2000 個字元。

程序

1. 按一下**攻擊**標籤。
2. 導覽至您要新增附註的攻擊。
3. 按兩下攻擊。
4. 從**動作**清單框中，選取**新增附註**。
5. 鍵入您要爲此攻擊包含的附註。
6. 按一下**新增附註**。

結果

附註會顯示在「攻擊」摘要的「最後 5 個附註」窗格中。 **附註**圖示會顯示在**攻擊**清單的旗標直欄中。如果您將滑鼠移至**攻擊**清單的**旗標**直欄中的附註指示器上，畫面上會顯示該攻擊的附註。

隱藏攻擊

若要避免攻擊顯示於**攻擊**標籤上，您可以隱藏攻擊。

關於這項作業

隱藏攻擊之後，攻擊將不再顯示於**攻擊**標籤上的任何清單內（例如，所有攻擊）；但是，如果您執行包含所隱藏之攻擊的搜尋，則該項目會顯示於搜尋結果內。

程序

1. 按一下**攻擊**標籤。
2. 按一下**所有攻擊**。
3. 選取您要隱藏的攻擊。
4. 從**動作**清單框中，選取**隱藏**。
5. 按一下**確定**。

顯示隱藏的攻擊

在**攻擊**標籤上看不到隱藏的攻擊，但是，如果要重新檢視它們，您可以顯示隱藏的攻擊。

關於這項作業

若要顯示隱藏的攻擊，則必須執行包含隱藏攻擊的搜尋。 搜尋結果包含所有攻擊，包括隱藏和非隱藏攻擊。 在**標示**欄中透過**隱藏**圖示將攻擊指定爲隱藏。

程序

1. 按一下**攻擊**標籤。
2. 按一下**所有攻擊**。
3. 搜尋隱藏的攻擊：
   a. 從**搜尋**清單框中，選取**新搜尋**。
   b. 在「搜尋參數」窗格上的**排除選項**清單中，清除**隱藏攻擊**勾選框。
   c. 按一下**搜尋**。
4. 找到並選取要顯示的隱藏攻擊。
5. 從**動作**清單框中，選取**顯示**。

關閉攻擊

若要從系統完全移除攻擊，您可以關閉攻擊。

關於這項作業

在您關閉（刪除）攻擊之後，攻擊不再顯示在**攻擊**標籤上的任何清單（例如，「所有攻擊」）中。攻擊保留期過後，關閉的攻擊會從資料庫中移除。 預設攻擊保留期爲三

天。 如果攻擊發生更多事件，會建立新的攻擊。 如果您執行包含關閉的攻擊的搜尋，搜尋結果中會顯示此項目（如果它尚未從資料庫中移除）。

關閉攻擊時，您必須選取關閉攻擊的原因，且可以新增附註。 **附註**欄位顯示爲先前關閉攻擊輸入的附註。 「附註」不得超過 2,000 個字元。此附註顯示在此攻擊的「附註」窗格中。 如果具有「管理攻擊關閉」許可權，您可以將新的自訂原因新增至**關閉原因**清單框。

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

程序

1. 按一下**攻擊**標籤。
2. 按一下**所有攻擊**。
3. 選擇下列其中一個選項：
   - 選取您要關閉的攻擊，然後從**動作**清單框中選取**關閉**。
   - 從**動作**清單框中，選取**關閉所列出的**。
4. 從**關閉原因**清單框中，選取原因。 預設原因爲**非問題**。
5. 選用項目。 在**附註**欄位中，鍵入附註以提供關閉附註的相關資訊。
6. 按一下**確定**。

結果

在您關閉攻擊之後，**攻擊**標籤的「依種類」窗格上顯示的計數可能需要數分鐘來反映關閉的攻擊。

保護攻擊

您可以阻止在保留期過後從資料庫移除攻擊。

關於這項作業

攻擊可以針對可配置的保留期進行保留。預設的保留期爲三天；但是，管理者可以自訂保留期。 您可能希望保留某些攻擊，而不考慮保留期。 您可以阻止在保留期過後從資料庫移除這些攻擊。

如需「攻擊保留期」的相關資訊，請參閱*IBM Security QRadar SIEM Administration Guide*。

注意：
當從「強迫清除」選項重設 SIM 資料模型時，會從資料庫和磁碟移除所有攻擊（包括受保護的攻擊）。 您必須具有管理專用權才能重設 SIM 資料模型。

程序

1. 按一下**攻擊**標籤。
2. 按一下**所有攻擊**。
3. 選擇下列其中一個選項：
   - 選取要保護的攻擊，然後從**動作**清單框選取**保護**。
   - 從**動作**清單框中，選取**保護所列項**。
4. 按一下**確定**。

結果

受保護的攻擊在**標示**欄內由**受保護**圖示指示。

解除保護攻擊

您可以在經過攻擊保留期之後解除保護之前阻止移除的攻擊。

關於這項作業

如果只列出受保護的攻擊，則可以執行搜尋只過濾受保護的攻擊。 如果清除**受保護**勾選框，並確定在「搜尋參數」窗格上的**排除選項**清單下選取了所有其他選項，則只顯示受保護的攻擊。

程序

1. 按一下**攻擊**標籤。
2. 按一下**所有攻擊**。
3. 選用項目。 執行搜尋僅顯示受保護的攻擊。
4. 選擇下列其中一個選項：
   - 選取要保護的攻擊，然後從「動作」清單框選取**解除保護**。
   - 從**動作**清單框中，選取**解除保護所列項**。
5. 按一下**確定**。

匯出攻擊

您可以用「延伸標記語言 (XML)」或「逗點區隔值 (CSV)」格式匯出攻擊。

關於這項作業

如果要重複使用或儲存攻擊資料，您可以匯出攻擊。 例如，您可以匯出攻擊以建立非 QRadar 產品型報告。 您也可以將攻擊匯出爲次要長期保留策略。 客戶支援中心可能會要求您匯出攻擊以用於疑難排解。

產生的 XML 或 CSV 檔案包含在搜尋參數的「直欄定義」窗格中指定的參數。 匯出資料所需的時間長度視指定的參數數目而定。

程序

1. 按一下**攻擊**標籤。
2. 在導覽功能表上，按一下**所有攻擊**。
3. 選取您要匯出的攻擊。
4. 選擇下列其中一個選項：
   - 若要以 XML 格式匯出攻擊，請從「動作」清單框中選取**動作 > 匯出至 XML**。
   - 若要以 CSV 格式匯出攻擊，請從「動作」清單框中選取**動作 > 匯出至 CSV**
5. 選擇下列其中一個選項：
   - 若要開啓清單以立即檢視，請選取**開啓工具**選項，然後從清單框中選取應用程式。
   - 若要儲存清單，請選取**儲存至磁碟**選項。
6. 按一下**確定**。

將攻擊指派給使用者

使用**攻擊**標籤，您可以將攻擊指派給使用者以進行調查。

關於這項作業

將攻擊指派給某位使用者時，「我的攻擊」頁面上會顯示屬於該使用者的攻擊。 您必須具有適當的專用權，才能將攻擊指派給使用者。

您可以透過**攻擊**標籤或「攻擊摘要」頁面將攻擊指派給使用者。此程序提供了有關如何透過**攻擊**標籤指派攻擊的指示。

註：使用者名稱清單框將僅顯示具有**攻擊**標籤專用權的使用者。

程序

1. 按一下**攻擊**標籤。
2. 按一下**所有攻擊**。
3. 選取您要指派的攻擊。
4. 從**動作**清單框中，選取**指派**。
5. 從**使用者名稱**清單框中，選取您要爲其指派此攻擊的使用者。
6. 按一下**儲存**。

結果

攻擊會指派給選取的使用者。 **使用者**圖示會顯示在**攻擊**標籤的「旗標」直欄中，以指示已指派攻擊。指定的使用者可以在「我的攻擊」頁面中查看此攻擊。

傳送電子郵件通知

您可以將包含攻擊摘要的電子郵件傳送至任何有效的電子郵件位址。

關於這項作業

電子郵件訊息的內文包含下列資訊（如果可用）：

- 來源 IP 位址
- 來源使用者名稱、主機名稱或資產名稱
- 來源總數
- 依長度列出的前五個來源
- 來源網路
- 目的地 IP 位址
- 目的地使用者名稱、主機名稱或資產名稱
- 目的地總數
- 依長度列出的前五個目的地
- 目的地網路
- 事件總數
- 導致攻擊或事件規則激發的規則
- 攻擊或事件規則的完整說明
- 攻擊 ID

- 前五個種類
- 攻擊的開始時間或事件產生時間
- 前五個註釋
- 攻擊使用者介面的鏈結
- 提出 CRE 規則

程序

1. 按一下**攻擊**標籤。
2. 導覽至您要傳送電子郵件通知的攻擊。
3. 按兩下攻擊。
4. 從**動作**清單框中，選取**電子郵件**。
5. 配置下列參數：

選項	敘述
參數	說明
收件者	鍵入在選取的攻擊發生變更時您要通知的使用者電子郵件位址。 使用逗點區隔多個電子郵件位址。
寄件者	鍵入預設起源電子郵件位址。 預設值爲 root@localhost.com。
電子郵件主旨	鍵入電子郵件的預設主旨。 預設值爲攻擊 ID。
電子郵件訊息	鍵入您要隨附通知電子郵件的標準訊息。

6. 按一下**傳送**。

將項目標示為追蹤

您可以使用**攻擊**標籤，將攻擊、來源 IP 位址、目的地 IP 位址與網路表示爲追蹤。這樣做將容許您追蹤特定項目，以便進一步調查。

程序

1. 按一下**攻擊**標籤。
2. 導覽至要標示爲追蹤的攻擊。
3. 按兩下攻擊。
4. 從**動作**清單框中，選取**追蹤**。

結果

現在，攻擊將會在**標示**欄內顯示一個標示，以指示攻擊標示爲追蹤。如果在攻擊清單上看不到標示的攻擊，則可以排列清單，以便首先顯示所有標示的攻擊。若要根據標示的攻擊來顯示攻擊清單，請按兩下**標示**欄標頭。

攻擊標籤工具列功能

攻擊標籤上的每個頁面及表格都有一個工具列，可爲您提供執行特定動作或調查攻擊的影響因素所需的功能。

表 13. 攻擊標籤工具列功能

功能	說明
新增附註	按一下**新增附註**，以將新附註新增至攻擊。 只有「攻擊摘要」頁面的「最後 5 個附註」窗格才提供此選項。
動作	**動作**清單框上可用的選項視頁面、表格或項目（如攻擊或來源 IP 位址）而定。 **動作**清單框可能與下面所示並不完全相同。 從**動作**清單框中，您可以選擇下列其中一個動作： • **追蹤** - 選取此選項可將項目標示爲進一步追蹤。 請參閱將項目標示爲追蹤。 • **隱藏** - 選取此選項可隱藏攻擊。如需隱藏攻擊的相關資訊，請參閱隱藏攻擊。 • **顯示** - 選取此選項可顯示所有隱藏的攻擊。 • **保護攻擊** - 選取此選項可保護攻擊。 如需保護攻擊的相關資訊，請參閱保護攻擊。 • **關閉** - 選取此選項可關閉攻擊。 如需關閉攻擊的相關資訊，請參閱關閉攻擊。 • **關閉列出的攻擊** - 選取此選項可關閉列出的攻擊。如需關閉列出的攻擊的相關資訊，請參閱關閉攻擊。 • **電子郵件** - 選取此選項可透過電子郵件將攻擊摘要傳送給一個以上收件者。 請參閱傳送電子郵件通知。 • **新增附註** - 選取此選項可將附註新增至項目。 請參閱新增附註。 • **指派** - 選取此選項可將攻擊指派給使用者。請參閱將攻擊指派給使用者。 • **列印** - 選取此選項可列印攻擊
註釋	按一下**註釋**，可檢視攻擊的所有註釋。 • **註釋** - 指定註釋的詳細資料。 註釋是規則可以自動新增至攻擊的文字說明（作爲規則回應的一部分新增）。 • **時間** - 指定建立註釋的日期和時間。
異常	按一下**異常**，可顯示導致異常偵測規則產生攻擊的已儲存搜尋結果。 **註**：只有在異常偵測規則產生攻擊時，才會顯示此按鈕。

表 13. 攻擊標籤工具列功能 (繼續)

功能	說明
種類	按一下**種類**，可檢視攻擊的種類資訊。 若要進一步調查與特定種類相關的事件，您也可以用滑鼠右鍵按一下種類，然後選取**事件**或**流程**。或者，您可以強調顯示種類，然後按一下「事件種類清單」工具列上的**事件**或**流程**圖示。
連線	按一下**連線**，可進一步調查連線。 **註：** 只有在您已購買 IBM Security QRadar Risk Manager 且獲得其授權時，此選項才可用。如需相關資訊，請參閱 *IBM Security QRadar Risk Manager User Guide*。 在您按一下**連線**圖示時，連線搜尋準則頁面會顯示在新頁面上，且已預先移入事件搜尋準則。 如果需要，您可以自訂搜尋參數。 按一下**搜尋**可檢視連線資訊。
目的地	按一下**目的地**，可檢視攻擊、來源 IP 位址或網路的所有本端目的地 IP 位址。 **註：** 如果目的地 IP 位址爲遠端，會開啓個別頁面，提供遠端目的地 IP 位址的資訊。
顯示	「攻擊摘要」頁面以多個表格形式顯示與攻擊相關的資訊。若要尋找表格，您可以捲動至您要檢視的表格，或從**顯示**清單框選取選項。
事件	按一下**事件**，可檢視攻擊的所有事件。 在您按一下**事件**時，畫面上會顯示事件搜尋結果。
流程	按一下**流程**，可進一步調查與攻擊相關聯的流程。 在您按一下**流程**時，畫面上會顯示流程搜尋結果。
日誌來源	按一下**日誌來源**，可檢視攻擊的所有日誌來源。
網路	按一下**網路**，可檢視攻擊的所有目的地網路。
附註	按一下**附註**，可檢視攻擊、來源 IP 位址、目的地 IP 位址或網路的所有附註。 如需附註的相關資訊，請參閱新增附註
攻擊	按一下**攻擊**，可檢視與來源 IP 位址、目的地 IP 位址或網路相關聯的攻擊清單。
列印	按一下**列印**，可列印攻擊。

表 13. 攻擊標籤工具列功能 (繼續)

功能	說明
規則	按一下**規則**，可檢視促成攻擊的所有規則。 會先列出建立攻擊的規則。 如果您具有適當的許可權來編輯規則，請按兩下規則以啓動「編輯規則」頁面。 如果規則已刪除，規則旁邊會顯示紅色圖示 (x)。 如果您按兩下刪除的規則，畫面上會顯示一則訊息，指出規則不再存在。
儲存準則	在您執行攻擊搜尋之後，按一下**儲存準則**可儲存您的搜尋準則以供將來使用。
儲存佈置	依預設，「依種類詳細資料」頁面會依「攻擊計數」參數排序。 如果您變更排序順序或依不同的參數排序，可按一下**儲存佈置**以將現行顯示儲存爲您的預設視圖。 下次您登入**攻擊**標籤時，畫面上會顯示已儲存的佈置。
搜尋	只有「本端目的地清單」表格工具列上才提供此選項。 按一下**搜尋**，可針對來源 IP 位址過濾目的地 IP。 若要過濾目的地： 1. 按一下**搜尋**。 2. 輸入下列參數的值： • **目的地網路** - 從清單框中，選取您要過濾的網路。 • **長度** - 從清單框中，選取您要針對「等於」、「小於」或「大於」配置值的長度■行過濾。 • **排序方式** - 從清單框中，選取您要排序過濾結果的方式。 3. 按一下**搜尋**。
顯示非作用中的種類	在「依種類詳細資料」頁面上，從低階種類中的值中累計每個種類的計數。 畫面上會顯示與攻擊相關聯的低階種類，其中含有箭頭。 您可以按一下箭頭來檢視相關聯的低階種類。 如果要檢視所有種類，請按一下**顯示非作用中的種類**。
來源	按一下**來源**，可檢視攻擊、目的地 IP 位址或網路的所有來源 IP 位址。
摘要	如果已按一下**顯示**清單框中的選項，您可以按一下**摘要**以回到詳細的摘要視圖。
使用者	按一下**使用者**，可檢視與攻擊相關聯的所有使用者。

表 13. 攻擊標籤工具列功能 (繼續)

功能	說明
檢視攻擊路徑	按一下**檢視攻擊路徑**，可進一步調查攻擊的攻擊路徑。 在您按一下**檢視攻擊路徑**圖示時，新頁面上會顯示「現行拓蹼」頁面。 **註**：只有在您已購買 IBM Security QRadar Risk Manager 且獲得其授權時，此選項才可用。如需相關資訊，請參閱 *IBM Security QRadar Risk Manager User Guide*。
檢視拓蹼	按一下**檢視拓蹼**，可進一步調查攻擊的來源。在您按一下**檢視拓蹼**圖示時，新頁面上會顯示「現行拓蹼」頁面。 **註**：只有在您已購買 IBM Security QRadar Risk Manager 且獲得其授權時，此選項才可用。 如需相關資訊，請參閱 *IBM Security QRadar Risk Manager User Guide*。

攻擊參數

此表提供「攻擊」標籤上提供的參數說明。

表 14. 攻擊參數

參數	位置	說明
註釋	「前 5 個註釋」表格	指定註釋的詳細資料。 註釋是規則可以自動新增至攻擊的文字說明（作爲規則回應的一部分新增）。
異常	「最後 10 個事件（異常事件）」表格	選取此選項可顯示導致異常偵測規則產生事件的已儲存搜尋結果。
異常文字	「最後 10 個事件（異常事件）」表格	指定異常偵測規則偵測到的異常行爲的說明。
異常值	「最後 10 個事件（異常事件）」表格	指定導致異常偵測規則產生攻擊的值。
應用程式	「最後 10 個流程」表格	指定與流程相關聯的應用程式。
應用程式名稱	「攻擊來源」表格（如果「攻擊類型」爲「應用程式 ID」）	指定與建立攻擊的流程相關聯的應用程式。
ASN 索引	「攻擊來源」表格（如果「攻擊類型」爲「來源 ASN」或「目的地 ASN」）	指定與建立攻擊的流程相關聯的 ASN 值。
資產名稱	「攻擊來源」表格（如果「攻擊類型」爲「來源 IP」或「目的地 IP」）	指定資產名稱，您可以使用「資產設定檔」功能來指派。如需相關資訊，請參閱資產管理。

表 14. 攻擊參數 (繼續)

參數	位置	說明
資產加權	「攻擊來源」表格（如果「攻擊類型」爲「來源 IP」或「目的地 IP」）	指定資產加權，您可以使用「資產設定檔」功能來指派。如需相關資訊，請參閱資產管理。
指派給	「攻擊」表格	指定指派給攻擊的使用者。 如果未指派使用者，此欄位會指定「未指派」。請按一下「未指派」以將攻擊指派給使用者。 如需相關資訊，請參閱將攻擊指派給使用者。
種類	「最後 10 個事件」表格	指定事件的種類。
種類名稱	「依種類詳細資料」頁面	指定高階種類名稱。
已鏈結	• 「攻擊來源」表格（如果「攻擊類型」爲「目的地 IP」） • 「前 5 個目的地 IP」表格	指定是否鏈結目的地 IP 位址。 已鏈結的目的地 IP 位址與其他攻擊相關聯。 例如，目的地 IP 位址可能會成爲其他攻擊的來源 IP 位址。 如果目的地 IP 位址已鏈結，請按一下**是**以檢視已鏈結的攻擊。
建立日期	「最後 5 個附註」表格	指定建立附註的日期和時間。
可靠性	「攻擊」表格	指定攻擊的可靠性，由來源裝置的可靠性等級判定。 例如，在多個攻擊報告相同事件或流程時，會增加可靠性。
現行搜尋參數	• 「依來源 IP 詳細資料」頁面 • 「依目的地 IP 詳細資料」頁面	表格頂端顯示套用到搜尋結果的搜尋參數的詳細資料。 若要清除這些搜尋參數，請按一下**清除過濾器**。 **註**：僅當套用過濾器之後才會顯示這個參數。
說明	• 「所有攻擊」頁面 • 「我的攻擊」頁面 • 「攻擊」表格 • 「依來源 IP - 攻擊清單」頁面 • 「依網路 - 攻擊清單」頁面 • 「依目的地 IP - 攻擊清單」頁面 • 「攻擊來源」表格（如果「攻擊類型」爲「日誌來源」） • 「前 5 個日誌來源」表格	指定攻擊或日誌來源的說明。

表 14. 攻擊參數 (繼續)

參數	位置	說明
目的地 IP	• 「最後 10 個事件」表格 • 「最後 10 個流程」表格	指定事件或流程的目的地 IP 位址。
目的地 IP	• 「前 5 個目的地 IP」表格 • 「依來源 IP - 本端目的地清單」頁面 • 「依目的地 IP 詳細資料」頁面 • 「依網路 - 本端目的地清單」頁面	指定目的地的 IP 位址。如果已在「管理」標籤上啓用「DNS 查閱」，您可以將滑鼠移在 IP 位址上方來檢視 DNS 名稱。
目的地 IP	「攻擊」表格	指定本端或遠端目的地的 IP 位址及資產名稱（如果可用）。按一下鏈結可檢視相關詳細資料。
目的地 IP	• 「所有攻擊」頁面 • 「我的攻擊」頁面	指定本端或遠端目的地的 IP 位址及資產名稱（如果可用）。如果多個目的地 IP 位址與攻擊相關聯，此欄位會指定「多個」及目的地 IP 位址的數目。
目的地 IP	• 「依來源 IP - 攻擊清單」頁面 • 「依網路 - 攻擊清單」頁面 • 「依目的地 IP - 攻擊清單」頁面	指定與攻擊相關聯的目的地的 IP 位址及資產名稱（如果可用）。如果已在「管理」標籤上啓用「DNS 查閱」，您可以將滑鼠移在 IP 位址或資產名稱上方來檢視 DNS 名稱。
目的地 IP	「依網路詳細資料」頁面	指定與網路相關聯的目的地 IP 位址的數目。
目的地埠	「最後 10 個流程」表格	指定流程的目的地埠。
目的地	• 「前 5 個來源 IP」表格 • 「依來源 IP 詳細資料」頁面 • 「依目的地 IP - 來源清單」頁面 • 「依網路 - 來源清單」頁面	指定 QID 對映中識別的事件名稱，它與建立攻擊的事件或流程相關聯。將滑鼠移在事件名稱上方，以檢視 QID。
事件/流程計數	「依種類詳細資料」頁面	指定與種類中的攻擊相關聯的作用中事件或流程（未關閉或隱藏的事件或流程）的數目。 如果未收到新事件或流程，攻擊僅會停留在作用中狀態一段時間。攻擊仍然會顯示在「攻擊」標籤上，但不會在此欄位中計數。

表 14. 攻擊參數 (繼續)

參數	位置	說明
事件/流程計數	目的地頁面 網路頁面	指定攻擊發生的事件和流程的數目，以及種類數目。 按一下事件鏈結，可進一步調查與攻擊相關聯的事件。 在您按一下事件鏈結時，畫面上會顯示事件搜尋結果。 按一下流程鏈結，可進一步調查與攻擊相關聯的流程。 在您按一下流程鏈結時，畫面上會顯示流程搜尋結果。 **註**：如果流程計數顯示 N/A，攻擊的開始日期可能早於您升級至 QRadar 產品 7.1.0 版 (MR1) 的日期。因此，流程無法計數。 但是，您可以按一下 N/A 鏈結來調查流程搜尋結果中的相關聯流程。
事件/流程計數	「依種類詳細資料」頁面	指定與種類中的攻擊相關聯的作用中事件或流程（未關閉或隱藏的事件或流程）的數目。 如果未收到新事件或流程，攻擊僅會停留在作用中狀態一段時間。攻擊仍然會顯示在「攻擊」標籤上，但不會在此欄位中計數。
事件/流程計數	目的地頁面 網路頁面	指定攻擊發生的事件和流程的數目，以及種類數目。 按一下事件鏈結，可進一步調查與攻擊相關聯的事件。 在您按一下事件鏈結時，畫面上會顯示事件搜尋結果。 按一下流程鏈結，可進一步調查與攻擊相關聯的流程。 在您按一下流程鏈結時，畫面上會顯示流程搜尋結果。 **註**：如果流程計數顯示 N/A，攻擊的開始日期可能早於您升級至 QRadar 產品 7.1.0 版 (MR1) 的日期。因此，流程無法計數。 但是，您可以按一下 N/A 鏈結來調查流程搜尋結果中的相關聯流程。

表 14. 攻擊參數 (繼續)

參數	位置	說明
事件	• 「所有攻擊」頁面 • 「我的攻擊」頁面 • 「依來源 IP - 攻擊清單」頁面 • 「依網路 - 攻擊清單」頁面 • 「依目的地 IP - 攻擊清單」頁面	指定攻擊的事件數目。
事件/流程	• 「攻擊來源」表格（如果「攻擊類型」爲「來源 IP」、「目的地 IP」、「主機名稱」、「使用者名稱」、「來源埠」或「目的地埠」、「事件名稱」、「埠」、「來源 MAC 位址」或「目的地 MAC 位址」、「日誌來源」、「來源 IPv6」或「目的地 IPv6」、「來源 ASN」或「目的地 ASN」、「規則」、「應用程式 ID」） • 「前 5 個來源 IP」表格 • 「依來源 IP 詳細資料」頁面 • 「依目的地 IP - 來源清單」頁面 • 「依網路 - 來源清單」頁面 • 「來源詳細資料」頁面 • 「前 5 個目的地 IP」表格 • 「依來源 IP - 本端目的地清單」頁面 • 「依目的地 IP 詳細資料」頁面 • 「依網路 - 本端目的地清單」頁面 • 「前 5 位使用者」表格 • 「前 5 個日誌來源」表格 • 「前 5 個種類」表格 • 「依網路詳細資料」頁面 • 「前 5 個種類」表格	指定與來源 IP 位址、目的地 IP 位址、事件名稱、使用者名稱、MAC 位址、日誌來源、主機名稱、埠、日誌來源、ASN 位址、IPv6 位址、規則、ASN、應用程式、網路或種類相關聯的事件或流程數目。按一下鏈結可檢視相關詳細資料。
看到第一個事件/流程的日期	「來源詳細資料」頁面	指定來源 IP 位址產生第一個事件或流程的日期和時間。

表 14. 攻擊參數 (繼續)

參數	位置	說明
旗標	• 「所有攻擊」頁面 • 「我的攻擊」頁面 • 「依來源 IP - 攻擊清單」頁面 • 「依網路 - 攻擊清單」頁面 • 「依目的地 IP - 攻擊清單」頁面	指出對攻擊執行的動作。 動作由下列圖示代表： • 旗標 - 指出將攻擊標示爲追蹤。 這可讓您追蹤特定項目以進一步調查。 如需如何將攻擊標示爲追蹤的相關資訊，請參閱將項目標示爲追蹤。 • 使用者 - 指出已將攻擊指派給使用者。將攻擊指派給某位使用者時，「我的攻擊」頁面上會顯示屬於該使用者的攻擊。如需將攻擊指派給使用者的相關資訊，請參閱將攻擊指派給使用者。 • 附註 - 指出使用者已將附註新增至攻擊。 「附註」可以包含您要爲攻擊擷取的任何資訊。 例如，您可以新增附註以指定未自動包含在攻擊中的資訊，如「客戶支援中心」通行證號碼或攻擊管理資訊。 如需新增附註的相關資訊，請參閱新增附註。 • 受保護 - 指出攻擊受保護。「保護」功能可防止指定的攻擊在保留期過後從資料庫中移除。 如需受保護攻擊的相關資訊，請參閱保護攻擊。 將滑鼠移在圖示上以顯示相關資訊。

表 14. 攻擊參數 (繼續)

參數	位置	說明
旗標（續）		• 非作用中的攻擊 - 指出這是非作用中的攻擊。 自攻擊收到最後一個事件五天後，攻擊會變成非作用中。 此外，在您升級 QRadar 產品軟體之後，所有攻擊都會變成非作用中。 非作用中的攻擊無法再變成作用中。 如果爲攻擊偵測到新事件，則會建立新攻擊，且會保留非作用中的攻擊，直到攻擊保留期已過。 您可以對非作用中的攻擊執行下列動作：保護、標示爲追蹤、新增附註及指派給使用者。
旗標	• 「依來源 IP 詳細資料」頁面 • 「依來源 IP - 本端目的地清單」頁面 • 「依目的地 IP 詳細資料」頁面 • 「依目的地 IP - 來源清單」頁面 • 「依網路詳細資料」頁面 • 「依網路 - 來源清單」頁面 • 「依網路 - 本端目的地清單」頁面	指定對來源 IP 位址、目的地 IP 位址或網路執行的動作。 例如，如果顯示旗標，則攻擊標示爲追蹤。 將滑鼠移在圖示上以顯示相關資訊。
流程	• 「所有攻擊」頁面 • 「我的攻擊」頁面 • 「依來源 IP - 攻擊清單」頁面 • 「依網路 - 攻擊清單」頁面 • 「依目的地 IP - 攻擊清單」頁面	指定攻擊的流程數目。 **註**：如果「流程」直欄顯示 N/A，攻擊的開始日期可能早於您升級至 QRadar 7.1.0 (MR1) 的日期。
分組	• 「攻擊來源」表格（如果「攻擊類型」爲「日誌來源」） • 「前 5 個日誌來源」表格	指定日誌來源所屬的群組。
群組	「攻擊來源」表格（如果「攻擊類型」爲「規則」）	指定規則所屬的規則群組。

表 14. 攻擊參數 (繼續)

參數	位置	說明
高階種類	「攻擊來源」表格（如果「攻擊類型」爲「事件名稱」）	指定事件的高階種類。 如需高階種類的相關資訊，請參閱 *IBM Security QRadar SIEM Administration Guide*。
主機名稱	「攻擊來源」表格（如果「攻擊類型」爲「來源 IP」或「目的地 IP」）	指定與來源或目的地 IP 位址相關聯的主機名稱。 如果未識別主機名稱，此欄位將指定「不明」。
歷程關聯設定檔名稱	• 攻擊摘要	指定建立攻擊之歷程關聯設定檔的名稱。
歷程關聯型錄	• 攻擊摘要	指定歷程關聯型錄，其包含觸發攻擊的事件。 若要查看型錄中的所有事件，請按一下「歷程關聯」視窗上的**檢視歷程**。
歷程關聯設定檔 ID	• 攻擊摘要	指定建立攻擊之歷程關聯設定檔的唯一 ID。
主機名稱	「攻擊來源」表格（如果「攻擊類型」爲「主機名稱」）	指定與建立攻擊的流程相關聯的主機名稱。
ID	• 「所有攻擊」頁面 • 「我的攻擊」頁面 • 「依來源 IP - 攻擊清單」頁面 • 「依網路 - 攻擊清單」頁面 • 「依目的地 IP - 攻擊清單」頁面 • 「依來源 IP - 攻擊清單」頁面 • 「依網路 - 攻擊清單」頁面	指定 QRadar 指派給攻擊的唯一識別號碼。
IP	• 「攻擊來源」表格（如果「攻擊類型」爲「來源 IP」或「目的地 IP」） • 「來源詳細資料」頁面	指定與建立攻擊的事件或流程相關聯的來源 IP 位址。
IP/DNS 名稱	「目的地」頁面	指定目的地的 IP 位址。如果已在**管理**標籤上啓用「DNS 查閱」，您可以將滑鼠移在 IP 位址或資產名稱上方來檢視 DNS 名稱。 如需相關資訊，請參閱 *IBM Security QRadar SIEM Administration Guide*。

表 14. 攻擊參數 (繼續)

參數	位置	說明
IPv6	「攻擊來源」表格（如果「攻擊類型」爲「來源 IPv6」或「目的地 IPv6」）	指定與建立攻擊的事件或流程相關聯的 IPv6 位址。
最後一個事件/流程	• 「所有攻擊」頁面 • 「我的攻擊」頁面 • 「依來源 IP - 本端目的地清單」頁面 • 「前 5 個來源 IP」表格 • 「依來源 IP 詳細資料」頁面 • 「依網路 - 來源清單」頁面 • 「前 5 個目的地 IP」表格 • 「依目的地 IP 詳細資料」頁面 • 「依目的地 IP - 來源清單」頁面 • 「依網路 - 本端目的地清單」頁面 • 「前 5 個種類」表格	指定自針對攻擊、種類、來源 IP 位址或目的地 IP 位址觀察最後一個事件或流程以來的經歷時間。
看到最後一個事件/流程的日期	「來源詳細資料」頁面	指定與來源 IP 位址相關聯的最後產生的事件或流程的日期和時間。
最後一個事件/流程時間	「攻擊來源」表格（如果「攻擊類型」爲「日誌來源」）	指定在系統上最後一次觀察日誌來源的日期和時間。
最後一個已知的群組	「攻擊來源」表格（如果「攻擊類型」爲「使用者名稱」、「來源 MAC 位址」、「目的地 MAC 位址」或「主機名稱」）	指定使用者、MAC 位址或主機名稱所屬的現行群組。 如果未關聯任何群組，則此欄位的值爲「不明」。 **註**：此欄位不顯示歷程資訊。
最後一個已知的主機	「攻擊來源」表格（如果「攻擊類型」爲「使用者名稱」、「來源 MAC 位址」或「目的地 MAC 位址」）	指定使用者或 MAC 位址與之相關聯的現行主機。 如果未識別主機，此欄位將指定「不明」。 **註**：此欄位不顯示歷程資訊。
最後一個已知的 IP	「攻擊來源」表格（如果「攻擊類型」爲「使用者名稱」、「來源 MAC 位址」、「目的地 MAC 位址」或「主機名稱」）	指定使用者、MAC 或主機名稱的現行 IP 位址。 如果未識別 IP 位址，此欄位將指定「不明」。 **註**：此欄位不顯示歷程資訊。
最後一個已知的 MAC	「攻擊來源」表格（如果「攻擊類型」爲「使用者名稱」或「主機名稱」）	指定使用者或主機名稱的最後一個已知 MAC 位址。 如果未識別 MAC，此欄位將指定「不明」。 **註**：此欄位不顯示歷程資訊。

表 14. 攻擊參數 (繼續)

參數	位置	說明
最後一個已知的機器	「攻擊來源」表格（如果「攻擊類型」爲「使用者名稱」、「來源 MAC 位址」、「目的地 MAC 位址」或「主機名稱」）	指定與使用者、MAC 位址或主機名稱相關聯的現行機器名稱。 如果未識別機器名稱，此欄位將指定「不明」。 **註**：此欄位不顯示歷程資訊。
最後一個已知的使用者名稱	「攻擊來源」表格（如果「攻擊類型」爲「來源 MAC 位址」、「目的地 MAC 位址」或「主機名稱」）	指定 MAC 位址或主機名稱的現行使用者。 如果未識別 MAC 位址，此欄位將指定「不明」。 **註**：此欄位不顯示歷程資訊。
最後一次觀察	「攻擊來源」表格（如果「攻擊類型」爲「使用者名稱」、「來源 MAC 位址」、「目的地 MAC 位址」或「主機名稱」）	指定在系統上最後一次觀察使用者、MAC 位址或主機名稱的日期和時間。
最後一次封包時間	「最後 10 個流程」表格	指定傳送流程的最後一個封包的日期和時間。
本端目的地計數	「前 5 個種類」表格 「依種類詳細資料」頁面	指定與種類相關聯的本端目的地 IP 位址數目。
本端目的地	「來源詳細資料」頁面	指定與來源 IP 位址相關聯的本端目的地 IP 位址。 若要檢視目的地 IP 位址的相關資訊，請按一下顯示的 IP 位址或術語。 如果存在多個目的地 IP 位址，畫面上會顯示術語「多個」。
位置	• 「攻擊來源」表格（如果「攻擊類型」爲「來源 IP」或「目的地 IP」） • 「前 5 個來源 IP」表格 • 「依來源 IP 詳細資料」頁面 • 「來源詳細資料」頁面 • 「依目的地 IP - 來源清單」頁面 • 「依網路 - 來源清單」頁面	指定來源 IP 位址或目的地 IP 位址的網路位置。 如果位置是本端，您可以按一下鏈結以檢視網路。
日誌來源	「最後 10 個事件」表格	指定偵測到事件的日誌來源。
日誌來源 ID	「攻擊來源」表格（如果「攻擊類型」爲「日誌來源」）	指定日誌來源的主機名稱。

表 14. 攻擊參數 (繼續)

參數	位置	說明
日誌來源名稱	「攻擊來源」表格（如果「攻擊類型」爲「日誌來源」）	指定「日誌來源」表格中識別的日誌來源名稱，它與建立攻擊的事件相關聯。 **註**：針對日誌來源攻擊顯示的資訊衍生自「管理」標籤上的「日誌來源」頁面。 您必須具有管理存取權，才能存取「管理」標籤及管理日誌來源。 如需日誌來源管理的相關資訊，請參閱 *管理日誌來源手冊*。
日誌來源	• 「所有攻擊」頁面 • 「我的攻擊」頁面 • 「依來源 IP - 攻擊清單」頁面 • 「依網路 - 攻擊清單」頁面 • 「依目的地 IP - 攻擊清單」頁面	指定與攻擊相關聯的日誌來源。 如果多個日誌來源與攻擊相關聯，此欄位會指定「多個」及日誌來源數目。
低階種類	「攻擊來源」表格（如果「攻擊類型」爲「事件名稱」）	指定事件的低階種類。
MAC	• 「攻擊來源」表格（如果「攻擊類型」爲「來源 IP」或「目的地 IP」） • 「前 5 個來源 IP」表格 • 「前 5 個目的地 IP」表格 • 「依來源 IP 詳細資料」頁面 • 「依來源 IP - 本端目的地清單」頁面 • 「依目的地 IP 詳細資料」頁面 • 「依目的地 IP - 來源清單」頁面 • 「依網路 - 來源清單」頁面 • 「依網路 - 本端目的地清單」頁面	指定攻擊開始時的來源或目的地 IP 位址的 MAC 位址。 如果 MAC 位址不明，此欄位將指定「不明」。
MAC 位址	「攻擊來源」表格（如果「攻擊類型」爲「來源 MAC 位址」或「目的地 MAC 位址」）	指定與建立攻擊的事件相關聯的 MAC 位址。 如果未識別 MAC 位址，此欄位將指定「不明」。

表 14. 攻擊參數 (繼續)

參數	位置	說明
長度	• 「所有攻擊」頁面 • 「我的攻擊」頁面 • 「攻擊」表格 • 「依來源 IP - 攻擊清單」頁面 • 「依網路 - 攻擊清單」頁面 • 「依目的地 IP - 攻擊清單」頁面 • 「前 5 個種類」表格 • 「最後 10 個事件」表格 • 「依網路詳細資料」頁面 • 網路頁面	指定攻擊、種類、事件或網路的相對重要性。 長度列以視覺方式呈現所有關聯的變數。 變數包括「關聯」、「嚴重性」及「可靠性」。 將滑鼠移在長度列上以顯示值及計算的長度。
長度	• 「攻擊來源」表格（如果「攻擊類型」爲「來源 IP」或「目的地 IP」） • 「前 5 個來源 IP」表格 • 「前 5 個目的地 IP」表格 • 「依來源 IP 詳細資料」頁面 • 「來源詳細資料」頁面 • 「依來源 IP - 本端目的地清單」頁面 • 「目的地」頁面 • 「依目的地 IP 詳細資料」頁面 • 「依目的地 IP - 來源清單」頁面 • 「依網路 - 來源清單」頁面 • 「依網路 - 本端目的地清單」頁面	指定來源或目的地 IP 位址的相對重要性。 長度列以視覺方式呈現與 IP 位址相關聯的資產的 CVSS 風險值。 將滑鼠移在長度列上以顯示計算的長度。
名稱	• 「前 5 個日誌來源」表格 • 「前 5 位使用者」表格 • 「前 5 個種類」表格 • 「網路」頁面	指定日誌來源的名稱、使用者、種類、網路 IP 位址或名稱。
網路	「依網路詳細資料」頁面	指定網路的名稱。

表 14. 攻擊參數 (繼續)

參數	位置	說明
網路	「攻擊」表格	指定攻擊的目的地網路。如果攻擊具有 1 個目的地網路，此欄位會顯示網路葉節點。 按一下鏈結可檢視網路資訊。 如果攻擊具有多個目的地網路，畫面上會顯示術語「多個」。按一下鏈結可檢視相關詳細資料。
附註	• 「攻擊來源」表格（如果「攻擊類型」爲「規則」） • 「最後 5 個附註」表格	指定規則的附註。
攻擊計數	「依種類詳細資料」頁面	指定每個種類中的作用中的攻擊數目。 作用中的攻擊是尚未隱藏或關閉的攻擊。 如果「依種類詳細資料」頁面包括「排除隱藏的攻擊」過濾器，則「攻擊計數」參數中顯示的攻擊計數可能不正確。如果您要在「依種類」窗格中檢視總數，請按一下「依種類詳細資料」頁面上「排除隱藏的攻擊」過濾器旁邊的**清除過濾器**。
攻擊來源	• 「所有攻擊」頁面 • 「我的攻擊」頁面 • 「依來源 IP - 攻擊清單」頁面 • 「依網路 - 攻擊清單」頁面 • 「依目的地 IP - 攻擊清單」頁面	指定攻擊來源的相關資訊。 **攻擊來源**欄位中顯示的資訊視攻擊類型而定。 例如，如果攻擊類型爲「來源埠」，則**攻擊來源**欄位會顯示建立攻擊的事件的來源埠。

表 14. 攻擊參數 (繼續)

參數	位置	說明
攻擊類型	• 「我的攻擊」頁面 • 「攻擊」表格 • 「依來源 IP - 攻擊清單」頁面 • 「依網路 - 攻擊清單」頁面 • 「依目的地 IP - 攻擊清單」頁面	指定攻擊類型。 「攻擊類型」是由建立攻擊的規則判定。 例如，如果攻擊類型爲日誌來源事件，則產生攻擊的規則會與基於裝置（偵測到事件的裝置）的事件產生關聯。 攻擊類型包括： • 來源 IP • 目的地 IP • 事件名稱 • 使用者名稱 • 來源 MAC 位址 • 目的地 MAC 位址 • 日誌來源 • 主機名稱 • 來源埠 • 目的地埠 • 來源 IPv6 • 目的地 IPv6 • 來源 ASN • 目的地 ASN • 規則 • 應用程式 ID 攻擊類型可判定「攻擊來源摘要」窗格上顯示的資訊類型。
攻擊	• 「來源詳細資料」頁面 • 「目的地」頁面	指定與來源或目的地 IP 位址相關聯的攻擊名稱。 若要檢視攻擊的相關資訊，請按一下顯示的名稱或術語。 如果存在多個攻擊，畫面上會顯示術語「多個」。
已啓動的攻擊	「網路」頁面	指定從網路啓動的攻擊。 如果多個攻擊可回應，此欄位會指定「多個」及攻擊數目。
已設定目標的攻擊	「網路」頁面	指定針對網路設定目標的攻擊。 如果多個攻擊可回應，此欄位會指定「多個」及攻擊數目

表 14. 攻擊參數 (繼續)

參數	位置	說明
攻擊	• 「攻擊來源」表格（如果「攻擊類型」爲「來源 IP」、「目的地 IP」、「事件名稱」、「使用者名稱」、「來源 MAC 位址」或「目的地 MAC 位址」、「日誌來源」、「主機名稱」、「來源埠」或「目的地埠」、「來源 IPv6」或「目的地 IPv6」、「來源 ASN」或「目的地 ASN」、「規則」、「應用程式 ID」） • 「前 5 個來源 IP」表格 • 「前 5 個目的地 IP」表格 • 「前 5 個日誌來源」表格 • 「前 5 位使用者」表格 • 「依來源 IP 詳細資料」頁面 • 「依來源 IP - 本端目的地清單」頁面 • 「依目的地 IP 詳細資料」頁面 • 「依目的地 IP - 來源清單」頁面 • 「依網路 - 來源清單」頁面 • 「依網路 - 本端目的地清單」頁面	指定與來源 IP 位址、目的地 IP 位址、事件名稱、使用者名稱、MAC 位址、日誌來源、主機名稱、埠、IPv6 位址、ASN、規則或應用程式相關聯的攻擊數目。 按一下鏈結可檢視相關詳細資料。
已啓動的攻擊	「依網路詳細資料」頁面	指定源於網路的攻擊數目。
已設定目標的攻擊	「依網路詳細資料」頁面	指定針對網路設定目標的攻擊數目。
埠	「攻擊來源」表格（如果「攻擊類型」爲「來源埠」或「目的地埠」）	指定與建立攻擊的事件或流程相關聯的埠。
關聯	「攻擊」表格	指定攻擊的相對重要性。
回應	「攻擊來源」表格（如果「攻擊類型」爲「規則」）	指定規則的回應類型。
規則說明	「攻擊來源」表格（如果「攻擊類型」爲「規則」）	指定規則參數的摘要。
規則名稱	「攻擊來源」表格（如果「攻擊類型」爲「規則」）	指定與建立攻擊的事件或流程相關聯的規則的名稱。 **註：**針對規則攻擊顯示的資訊衍生自**規則**標籤。

表 14. 攻擊參數 (繼續)

參數	位置	說明
規則類型	「攻擊來源」表格（如果「攻擊類型」爲「規則」）	指定攻擊的規則類型。
嚴重性	• 「攻擊來源」表格（如果「攻擊類型」爲「事件名稱」） • 「攻擊」表格	指定事件或攻擊的嚴重性。嚴重性指定攻擊造成的威脅程度，與目的地 IP 位址應對攻擊的程度相關。此值直接對映至與攻擊關聯的事件種類。 例如，「阻斷服務 (DoS)」攻擊的嚴重性爲 10，這指定嚴重的出現項目。
來源計數	「依種類詳細資料」頁面	指定與種類中攻擊相關聯的來源 IP 位址數目。 如果來源 IP 位址與五種不同的低階種類中的攻擊相關聯，則來源 IP 位址僅計數一次。
來源 IP	• 「依來源 IP 詳細資料」頁面 • 「依目的地 IP - 來源清單」頁面 • 「依網路 - 來源清單」頁面 • 「前 5 個來源 IP」表格 • 「最後 10 個流程」表格	指定已嘗試侵害網路上元件安全的裝置的 IP 位址或主機名稱。 如果已在「管理」標籤上啓用「DNS 查閱」，您可以將滑鼠移在 IP 位址上方來檢視 DNS 名稱。 如需相關資訊，請參閱 *IBM Security QRadar SIEM Administration Guide*。
來源 IP	「攻擊」表格	指定已嘗試侵害網路上元件安全的裝置的 IP 位址或主機名稱。 按一下鏈結可檢視相關詳細資料。 如需來源 IP 位址的相關資訊，請參閱監視依來源 IP 分組的攻擊。
來源 IP	• 「所有攻擊」頁面 • 「我的攻擊」頁面 • 「依來源 IP - 攻擊清單」頁面 • 「依網路 - 攻擊清單」頁面 • 「依目的地 IP - 攻擊清單」頁面	指定已嘗試侵害網路上元件安全的裝置的 IP 位址或主機名稱。 如果多個來源 IP 位址與攻擊相關聯，此欄位會指定「多個」及來源 IP 位址的數目。 如果已在「管理」標籤上啓用「DNS 查閱」，您可以將滑鼠移在 IP 位址或資產名稱上方來檢視 DNS 名稱。 如需相關資訊，請參閱 *IBM Security QRadar SIEM Administration Guide*。
來源 IP	「依網路詳細資料」頁面	指定與網路相關聯的來源 IP 位址的數目。

表 14. 攻擊參數 (繼續)

參數	位置	說明
來源埠	「最後 10 個流程」表格	指定流程的來源埠。
來源	• 「前 5 個目的地 IP」表格 • 「依來源 IP - 本端目的地清單」頁面 • 「依目的地 IP 詳細資料」頁面	指定目的地 IP 位址的來源 IP 位址的數目。
來源	• 「目的地」頁面 • 「網路」頁面	指定與目的地 IP 位址或網路相關聯的攻擊的來源 IP 位址。若要檢視來源 IP 位址的相關資訊，請按一下顯示的 IP 位址、資產名稱或術語。 如果指定單一來源 IP 位址，畫面上會顯示 IP 位址及資產名稱（如果可用）。 您可以按一下 IP 位址或資產名稱，來檢視來源 IP 位址詳細資料。 如果存在多個來源 IP 位址，此欄位會指定「多個」及來源 IP 位址的數目。
來源	「依網路 - 本端目的地清單」頁面	指定與目的地 IP 位址相關聯的來源 IP 位址的數目。
開始	「攻擊」表格	指定針對攻擊發生的第一個事件或流程的日期和時間。
開始日期	• 「所有攻擊」頁面 • 「我的攻擊」頁面 • 「依來源 IP - 攻擊清單」頁面 • 「依網路 - 攻擊清單」頁面 • 「依目的地 IP - 攻擊清單」頁面	指定與攻擊相關聯的第一個事件或流程的日期和時間。
狀態	「攻擊來源」表格（如果「攻擊類型」爲「日誌來源」）	指定日誌來源的狀態。

表 14. 攻擊參數 (繼續)

參數	位置	說明
狀態	「攻擊」表格	顯示圖示以指出攻擊狀態。 狀態圖示包括： **非作用中的攻擊**。自攻擊收到最後一個事件五天後，攻擊會變成非作用中。 在升級 QRadar 產品軟體之後，所有攻擊都會變成非作用中。 非作用中的攻擊無法再變成作用中。 如果爲攻擊偵測到新事件，則會建立新攻擊，且會保留非作用中的攻擊，直到攻擊保留期已過。 您可以對非作用中的攻擊進行下列動作：保護、標示爲追蹤、新增附註以及指派給使用者。 「所有攻擊」頁面上**隱藏的攻擊**旗標表示攻擊已隱藏，無法檢視。如果您搜尋隱藏的攻擊，它們只會顯示在將其標記爲隱藏的攻擊的「 所有攻擊」頁面上。 如需相關資訊，請參閱隱藏攻擊。 **使用者**指出攻擊指派給使用者。 將攻擊指派給某位使用者時，「我的攻擊」頁面上會顯示屬於該使用者的攻擊。 如需相關資訊，請參閱將攻擊指派給使用者。 **保護**可防止指定的攻擊在保留期過後從資料庫中移除。 如需相關資訊，請參閱保護攻擊。 **已關閉的攻擊**指出攻擊已關閉。 如需相關資訊，請參閱關閉攻擊。
時間	• 「最後 10 個事件」表格 • 「最後 10 個事件（異常事件）」表格	指定在正規化事件中偵測到第一個事件的日期和時間。 此日期和時間是由偵測到此事件的裝置指定。
時間	「前 5 個註釋」表格	指定建立註釋的日期和時間。
位元組總數	「最後 10 個流程」表格	指定流程的位元組總數。
事件/流程總數	• 「前 5 個日誌來源」表格 • 「前 5 位使用者」表格	指定日誌來源或使用者的事件總數。

表 14. 攻擊參數 (繼續)

參數	位置	說明
使用者	• 「攻擊來源」表格（如果「攻擊類型」爲「來源 IP」或「目的地 IP」，或是「使用者名稱」） • 「前 5 個來源 IP」表格 • 「前 5 個目的地 IP」表格 • 「依來源 IP 詳細資料」頁面 • 「依來源 IP - 本端目的地清單」頁面 • 「依目的地 IP 詳細資料」頁面 • 「依目的地 IP - 來源清單」頁面 • 「依網路 - 來源清單」頁面 • 「依網路 - 本端目的地清單」頁面	指定與來源 IP 位址或目的地 IP 位址相關聯的使用者。 如果未識別使用者，此欄位將指定「不明」。
使用者名稱	「攻擊來源」表格（如果「攻擊類型」爲「使用者名稱」）	指定與建立攻擊的事件或流程相關聯的使用者名稱。 **註**：如果您將滑鼠指標移到使用者名稱參數上，則顯示的工具提示會提供與「資產」標籤中的最近使用者名稱資訊相關聯的使用者名稱，而不是與建立攻擊的事件或流程相關聯的使用者名稱。
使用者名稱	「最後 5 個附註」表格	指定建立附註的使用者。
使用者	• 「所有攻擊」頁面 • 「我的攻擊」頁面 • 「依來源 IP - 攻擊清單」頁面 • 「依網路 - 攻擊清單」頁面 • 「依目的地 IP - 攻擊清單」頁面	指定與攻擊相關聯的使用者名稱。 如果多個使用者名稱與攻擊相關聯，此欄位會指定「多個」及使用者名稱數目。如果未識別使用者，此欄位將指定「不明」。
檢視攻擊	• 「依來源 IP 詳細資料」頁面 • 「依目的地 IP 詳細資料」頁面	從此清單框中選取選項，可過濾您要在此頁面上檢視的攻擊。 您可以檢視所有攻擊，或依基於時間範圍的攻擊進行過濾。 從清單框中，選取過濾所要依據的時間範圍。
漏洞	「攻擊來源」表格（如果「攻擊類型」爲「來源 IP」或「目的地 IP」）	指定與來源或目的地 IP 位址相關聯的所識別漏洞數目。 此值也包含主動及被動漏洞的數目。

表 14. 攻擊參數 (繼續)

參數	位置	說明
漏洞	「依目的地 IP - 來源清單」頁面	指定來源 IP 位址是否具有漏洞。
漏洞	• 「前 5 個來源 IP」表格 • 「依來源 IP 詳細資料」頁面 • 「依網路 - 來源清單」頁面 • 「前 5 個目的地 IP」表格 • 「依來源 IP - 本端目的地清單」頁面 • 「依目的地 IP 詳細資料」頁面 • 「依網路 - 本端目的地清單」頁面	指定來源或目的地 IP 位址是否具有漏洞。
加權	• 「前 5 個來源 IP」表格 • 「前 5 個目的地 IP」表格 • 「依來源 IP - 本端目的地清單」頁面 • 「依來源 IP 詳細資料」頁面 • 「依目的地 IP 詳細資料」頁面 • 「依目的地 IP - 來源清單」頁面 • 「依網路 - 來源清單」頁面 • 「依網路 - 本端目的地清單」頁面 • 「前 5 個註釋」表格	指定來源 IP 位址、目的地 IP 位址或註釋的加權。 IP 位址的加權在**資產**標籤上指派。 如需相關資訊，請參閱資產管理。

第 5 章 日誌活動調查

您可以即時監視及調查事件或執行進階搜尋。

使用**日誌活動**標籤，您可以即時監視及調查日誌活動（事件），或執行進階搜尋。

日誌活動標籤概觀

事件是來自日誌來源（如防火牆或路由器裝置）的記錄，用於說明對網路或主機的動作。

日誌活動標籤指定與攻擊相關聯的事件。

您必須具有檢視**日誌活動**標籤的許可權。

日誌活動標籤工具列

您可以從「日誌活動」工具列存取數個選項

使用工具列，您可以存取下列選項：

表 15. 日誌活動工具列選項

選項	說明
搜尋	按一下**搜尋**，可對事件執行進階搜尋。 選項包括： • **新建搜尋** - 選取此選項可建立新的事件搜尋。 • **編輯搜尋** - 選取此選項可選取及編輯事件搜尋。 • **管理搜尋結果** - 選取此選項可檢視及管理搜尋結果。
快速搜尋	從此清單框中，您可以執行先前儲存的搜尋。僅當您具有已儲存的搜尋準則來指定**包含在我的快速搜尋中**選項時，選項才會顯示在**快速搜尋**清單框中。
新增過濾器	按一下**新增過濾器**，可將過濾器新增至現行搜尋結果。
儲存準則	按一下**儲存準則**，可儲存現行搜尋準則。
儲存結果	按一下**儲存結果**，可儲存現行搜尋結果。 此選項僅在搜尋完成之後才會顯示。 在串流模式下，此選項會停用。
取消	按一下**取消**，可取消正在進行的搜尋。 在串流模式下，此選項會停用。

表 15. 日誌活動工具列選項 (繼續)

選項	說明
誤判	按一下**誤判**，可開啓「誤判調整」視窗，此視窗可讓您調除已知誤判的事件以防止建立攻擊。 在串流模式下，此選項會停用。 如需調整誤判的相關資訊，請參閱調整誤判。
規則	僅在您具有檢視規則的許可權時，才會顯示「規則」選項。 按一下**規則**，可配置自訂事件規則。 選項包括： • **規則** - 選取此選項可檢視或建立規則。 如果您僅具有檢視規則的許可權，畫面上會顯示「規則」精靈的摘要頁面。 如果您具有維護自訂規則的許可權，畫面上會顯示「規則」精靈，且您可以編輯規則。 若要啓用異常偵測規則選項（「新增臨界值規則」、「新增行爲規則」及「新增異常規則」），您必須儲存聚集的搜尋準則，因爲已儲存的搜尋準則會指定必要的參數。 **註**：僅在您具有**日誌活動 > 維護自訂規則**許可權時，才會顯示異常偵測規則選項。 • **新增臨界值規則** - 選取此選項可建立臨界值規則。 臨界值規則可針對超出所配置臨界值的活動測試事件資料流量。 臨界值可以基於 QRadar 收集的任何資料。例如，如果您建立臨界值規則，指出在 8 am 至 5 pm 之間登入伺服器的用戶端不能超過 220 個，則在第 221 個用戶端嘗試登入時，規則會產生警示。 在您選取**新增臨界值規則**選項時，畫面上會顯示「規則」精靈，且已預先移入用於建立臨界值規則的適當選項。

表 15. 日誌活動工具列選項 (繼續)

選項	說明
規則（續）	• **新增行為規則** - 選取此選項可建立行爲規則。 行爲規則會測試異常活動（例如存在新的或不明的資料流量）的事件資料流量，即突然停止或物件處於作用中狀態的時間量百分比變更的資料流量。例如，您可以建立行爲規則，將前 5 分鐘的平均資料流量與前一小時的平均資料流量進行比較。如果變更超過 40%，規則會產生回應。 在您選取**新增行為規則**選項時，畫面上會顯示「規則」精靈，且已預先移入用於建立行爲規則的適當選項。 • **新增異常規則** - 選取此選項可建立異常規則。 異常規則會測試異常活動（例如存在新的或不明的資料流量）的事件資料流量，即突然停止或物件處於作用中狀態的時間量百分比變更的資料流量。例如，如果永不與亞洲通訊的網路區域開始與該國家/地區中的主機通訊，異常規則會產生警示。 在您選取**新增異常規則**選項時，畫面上會顯示「規則」精靈，且已預先移入用於建立異常規則的適當選項。

表 15. 日誌活動工具列選項 (繼續)

選項	說明
動作	按一下**動作**可執行下列動作： • **全部顯示** - 選取此選項可移除搜尋準則上的所有過濾器，及顯示所有未過濾的事件。 • **列印** - 選取此選項可列印頁面上顯示的事件。 • **匯出至 XML > 可見的直欄** - 選取此選項，可僅匯出在「日誌活動」標籤上顯示的直欄。 這是建議的選項。 請參閱「匯出事件」。 • **匯出至 XML > 完全匯出（全部直欄）** - 選取此選項可匯出所有事件參數。 完全匯出可能需要較長時間才能完成。請參閱匯出事件。 • **匯出至 CSV > 可見的直欄** - 選取此選項，可僅匯出在「日誌活動」標籤上顯示的直欄。 這是建議的選項。 請參閱匯出事件。 • **匯出至 CSV > 完全匯出（全部直欄）** - 選取此選項可匯出所有事件參數。 完全匯出可能需要較長時間才能完成。 請參閱匯出事件。 • **刪除** - 選取此選項可刪除搜尋結果。 請參閱管理事件及流程搜尋結果。 • **通知** - 選取此選項，可指定您要在完成選取的搜尋時獲得電子郵件通知。 此選項僅對正在進行的搜尋啓用。 **註**：在串流模式下以及在檢視部分搜尋結果時，**列印**、**匯出至 XML** 及**匯出至 CSV** 選項會停用。
搜尋工具列	**進階搜尋** 從清單框中選取**進階搜尋**，以輸入 Ariel 查詢語言 (AQL) 搜尋字串來指定要傳回的欄位。 **快速過濾器** 從清單框中選取「快速過濾器」，以透過使用簡式字詞或片語來搜尋有效負載。
視圖	**日誌活動**標籤上的預設視圖是即時事件的串流。**視圖**清單包含一些選項，也可檢視指定時段中的事件。在從**視圖**清單中選擇指定的時段之後，您就可以變更**開始時間**及**結束時間**欄位中的日期和時間值，來修改顯示的時段。

右鍵功能表選項

在**日誌活動**標籤上，您可以用滑鼠右鍵按一下事件以存取更多事件過濾器資訊。

右鍵功能表選項爲：

表 16. 右鍵功能表選項

選項	說明
過濾	選取此選項可過濾選取的事件，具體視事件中選取的參數而定。
誤判	選取此選項可開啓「誤判」視窗，此視窗將讓您調除已知誤判的事件以防止建立攻擊。 在串流模式下，此選項會停用。請參閱調整誤判。
其他選項：	選取此選項可調查 IP 位址或使用者名稱。 如需調查 IP 位址的相關資訊，請參閱「調查 IP 位址」。 如需調查使用者名稱的相關資訊，請參閱調查使用者名稱。 **註**：在串流模式下，不會顯示此選項。
快速過濾器	過濾符合或不符合選取項目的項目。

狀態列

串流事件時，狀態列會顯示每秒收到的平均結果數目。

這是主控台成功從事件處理器收到的結果數目。 如果每秒此數目超過 40 個結果，畫面上僅顯示 40 個結果。 餘數會累計在結果緩衝區中。 若要檢視更多狀態資訊，請將滑鼠指標移在狀態列上。

未串流事件時，狀態列顯示目前顯示在標籤上的搜尋結果數目及處理搜尋結果所需的時間量。

日誌活動監視

依預設，**日誌活動**標籤會在串流模式下顯示事件，以容許您即時檢視事件。

如需串流模式的相關資訊，請參閱檢視串流事件。 您可以使用**視圖**清單框，以指定不同的時間範圍來過濾事件。

如果您先前已將儲存的搜尋準則配置爲預設值，則存取**日誌活動**標籤時，會自動顯示該搜尋的結果。 如需儲存搜尋準則的相關資訊，請參閱儲存事件及流程搜尋準則。

檢視串流事件

串流模式將容許您檢視進入系統的事件資料。 此模式爲您提供現行事件活動的即時視圖，顯示前 50 個事件。

關於這項作業

如果在啓用串流模式之前，您在**日誌活動**標籤上或搜尋準則中套用了任何過濾器，則會以串流模式保留過濾器。 但是，串流模式不支援包括分組事件的搜尋。 如果對分組事件或分組搜尋準則啓用串流模式，則**日誌活動**標籤會顯示正規化事件。 請參閱檢視正規化事件。

當您要選取事件以檢視詳細資料或執行動作時，必須先暫停串流，才能按兩下事件。 暫停串流時，會顯示前 1000 個事件。

程序

1. 按一下**日誌活動**標籤。
2. 從**檢視**清單框中，選取**即時（串流）**。 如需工具列選項的相關資訊，請參閱表 4-1。 如需以串流模式顯示參數的相關資訊，請參閱表 4-7。
3. 選用項目。 暫停或播放串流事件。 選擇下列其中一個選項：
   - 若要選取事件記錄，請按一下**暫停**圖示以暫停串流。
   - 若要重新啓動串流模式，請按一下**播放**圖示。

檢視正規化事件

事件以原始格式收集，然後經正規化才能顯示在**日誌活動**標籤上。

關於這項作業

正規化涉及剖析未處理的事件資料，及準備資料以顯示可讀的標籤相關資訊。 若正規化事件，則系統還將正規化名稱。 所以，在**日誌活動**標籤上顯示的名稱可能與事件中顯示的名稱不符。

註：如果選取要顯示的時間範圍，則會顯示時間序列圖表。如需使用時間序列圖表的相關資訊，請參閱時間序列圖表概觀。

當您檢視正規化事件時，**日誌活動**標籤顯示下列參數：

表 17. 「日誌活動」標籤 - 預設（正規化）參數

參數	說明
Current®過濾器	此表格頂端顯示套用到搜尋結果的過濾器的詳細資料。 若要清除這些過濾器值，請按一下**清除過濾器**。 **註**：僅當套用過濾器之後才會顯示這個參數。
檢視	從這個清單框中，您可以選取要過濾的時間範圍。

表 17. 「日誌活動」標籤 - 預設（正規化）參數 (繼續)

參數	說明
現行統計資料	當未使用「即時（串流）」或「前一分鐘（自動重新整理）」模式時，會顯示現行統計資料，包括： **註**：按一下**現行統計資料**旁的箭頭，以顯示或隱藏統計資料。 • **結果總計** - 指定符合搜尋準則的結果總數。 • **已搜尋的資料檔案** - 指定在指定期間跨距內已搜尋的資料檔案總數。 • **已搜尋的壓縮資料檔案** - 指定在指定期間跨距內已搜尋的壓縮資料檔案總數。 • **索引檔案計數** - 指定在指定期間跨距內已搜尋的索引檔案總數。 • **持續時間** - 指定搜尋的持續時間。 **註**：現行統計資料有助於進行疑難排解。 當您聯絡客戶支援中心，以對事件進行疑難排解時，可能會被要求提供現行統計資訊。
圖表	顯示可配置圖表，以代表符合時間間隔與分組選項的記錄。如果要從顯示畫面中移除圖表，按一下**隱藏圖表**。 僅當您選取「前次間隔（自動重新整理）」或以上的時間範圍，以及要顯示的分組選項時，才會顯示圖表。 如需配置圖表的相關資訊，請參閱圖表管理。 **註**：如果您使用 Mozilla Firefox 作爲瀏覽器，並安裝了廣告封鎖程式瀏覽器延伸，則不顯示圖表。若要顯示圖表，則必須移除廣告封鎖程式瀏覽器延伸。如需相關資訊，請參閱瀏覽器說明文件。
攻擊圖示	按一下此圖示，以檢視與此事件相關聯的攻擊的詳細資料。 如需相關資訊，請參閱圖表管理。 **註**：視您的產品而定，此圖示可能無法使用。您必須具有 IBM Security QRadar SIEM。
開始時間	指定第一個事件的時間（由日誌來源報告至 QRadar）。
事件名稱	指定事件的正規化名稱。
日誌來源	指定引起事件的日誌來源。 如果有多個日誌來源與此事件相關聯，則此欄位指定術語「多個」，以及日誌來源的數目。
事件計數	指定此正規化事件中處理的事件總數。 若在短時間內偵測到相同來源及目的地 IP 位址有多個相同類型的事件，則會將這些事件組合起來。
時間	指定 QRadar 接收事件的日期和時間。
低階種類	指定與此事件相關聯的低階種類。 如需事件種類的相關資訊，請參閱*IBM Security QRadar SIEM Administration Guide*。

表 17. 「日誌活動」標籤 - 預設（正規化）參數 (繼續)

參數	說明
來源 IP	指定事件的來源 IP 位址。
來源埠	指定事件的來源埠。
目的地 IP	指定事件的目的地 IP 位址。
目的地埠	指定事件的目的地埠。
使用者名稱	指定與此事件相關聯的使用者名稱。 在鑒別相關的事件中一般可以使用使用者名稱。 對於無法使用使用者名稱的所有其他類型事件，此欄位指定 N/A。
長度	指定此事件的長度。 變數包括可靠性、相關性與嚴重性。 將您的滑鼠移至長度列，以顯示值及計算的長度。

程序

1. 按一下**日誌活動**標籤。
2. 從**顯示**清單框中，選取**預設（正規化）**。
3. 從**檢視**清單框中，選取要顯示的時間範圍。
4. 按一下**暫停**圖示，以暫停串流。
5. 按兩下要進一步檢視明細的事件。 如需相關資訊，請參閱事件明細。

檢視未處理的事件

您可以從日誌來源檢視未處理的事件資料，即未剖析的事件資料。

關於這項作業

當您檢視未處理的事件資料時，**日誌活動**標籤提供每一個事件的下列參數。

表 18. 未處理的事件參數

參數	說明
現行過濾器	此表格頂端顯示套用到搜尋結果的過濾器的詳細資料。 若要清除這些過濾器值，請按一下**清除過濾器**。 **註**：僅當套用過濾器之後才會顯示這個參數。
檢視	從這個清單框中，您可以選取要過濾的時間範圍。

表 18. 未處理的事件參數 (繼續)

參數	說明
現行統計資料	當未使用「即時（串流）」或「前一分鐘（自動重新整理）」模式時，會顯示現行統計資料，包括： **註**：按一下**現行統計資料**旁的箭頭，以顯示或隱藏統計資料。 • **結果總計** - 指定符合搜尋準則的結果總數。 • **已搜尋的資料檔案** - 指定在指定期間跨距內已搜尋的資料檔案總數。 • **已搜尋的壓縮資料檔案** - 指定在指定期間跨距內已搜尋的壓縮資料檔案總數。 • **索引檔案計數** - 指定在指定期間跨距內已搜尋的索引檔案總數。 • **持續時間** - 指定搜尋的持續時間。 **註**： 現行統計資料有助於進行疑難排解。當您聯絡客戶支援中心，以對事件進行疑難排解時，可能會被要求提供現行統計資訊。
圖表	顯示可配置圖表，以代表符合時間間隔與分組選項的記錄。如果要從顯示畫面中移除圖表，按一下**隱藏圖表**。 僅當您選取「前次間隔（自動重新整理）」或以上的時間範圍，以及要顯示的分組選項時，才會顯示圖表。 **註**：如果您使用 Mozilla Firefox 作爲瀏覽器，並安裝了廣告封鎖程式瀏覽器延伸，則不顯示圖表。若要顯示圖表，則必須移除廣告封鎖程式瀏覽器延伸。如需相關資訊，請參閱瀏覽器說明文件。
攻擊圖示	按一下此圖示，以檢視與此事件相關聯的攻擊的詳細資料。
開始時間	指定第一個事件的時間（由日誌來源報告至 QRadar）。
日誌來源	指定引起事件的日誌來源。 如果有多個日誌來源與此事件相關聯，則此欄位指定術語「多個」，以及日誌來源的數目。
有效負載	以 UTF-8 格式指定原始事件有效負載資訊。

程序

1. 按一下**日誌活動**標籤。
2. 從**顯示**清單框中，選取**未處理的事件**。
3. 從**檢視**清單框中，選取要顯示的時間範圍。
4. 按兩下要進一步檢視明細的事件。 請參閱事件明細。

檢視分組事件

您可以使用**日誌活動**標籤，檢視依各種選項分組的事件。 從**顯示**清單框中，可以選取作爲事件分組依據的參數。

關於這項作業

「顯示」清單框不會以串流模式顯示，因爲串流模式不支援分組事件。 如果使用未分組的搜尋準則進入串流模式，則會顯示此選項。

「顯示」清單框提供下列選項：

表 19. 分組事件選項

分組選項	說明
低階種類	顯示依事件的低階種類分組的事件彙總清單。 如需種類的相關資訊，請參閱 *IBM Security QRadar SIEM Administration Guide*。
事件名稱	顯示依事件的正規化名稱分組的事件彙總清單。
目的地 IP	顯示依事件的目的地 IP 位址分組的事件彙總清單。
目的地埠	顯示依事件的目的地埠位址分組的事件彙總清單。
來源 IP	顯示依事件的來源 IP 位址分組的事件彙總清單。
自訂規則	顯示依關聯的自訂規則分組的事件彙總清單。
使用者名稱	顯示依事件關聯的使用者名稱分組的事件彙總清單。
日誌來源	顯示依將事件傳送給 QRadar 的日誌來源分組的事件彙總清單。
高階種類	顯示依事件的高階種類分組的事件彙總清單。
網路	顯示依事件關聯的網路分組的事件彙總清單。
來源埠	顯示依事件的來源埠位址分組的事件彙總清單。

從**顯示**清單框選取選項之後，資料的直欄佈置視所選群組選項而定。事件表格中的每一列代表一個事件群組。 **日誌活動**標籤提供每一個事件群組的下列資訊

表 20. 分組事件參數

參數	說明
分組依據	指定作爲搜尋分組依據的參數。
現行過濾器	此表格頂端顯示套用到搜尋結果的過濾器的詳細資料。 若要清除這些過濾器值，請按一下**清除過濾器**。
檢視	從清單框中，選取要過濾的時間範圍。

表 20. 分組事件參數 (繼續)

參數	說明
現行統計資料	當未使用「即時（串流）」或「前一分鐘（自動重新整理）」模式時，會顯示現行統計資料，包括： **註**：按一下**現行統計資料**旁的箭頭，以顯示或隱藏統計資料。 • **結果總計** - 指定符合搜尋準則的結果總數。 • **已搜尋的資料檔案** - 指定在指定期間跨距內已搜尋的資料檔案總數。 • **已搜尋的壓縮資料檔案** - 指定在指定期間跨距內已搜尋的壓縮資料檔案總數。 • **索引檔案計數** - 指定在指定期間跨距內已搜尋的索引檔案總數。 • **持續時間** - 指定搜尋的持續時間。 **註**：現行統計資料有助於進行疑難排解。 當您聯絡客戶支援中心，以對事件進行疑難排解時，可能會被要求提供現行統計資訊。
圖表	顯示可配置圖表，以代表符合時間間隔與分組選項的記錄。如果要從顯示畫面中移除圖表，按一下**隱藏圖表**。 每一個圖表提供一個圖註，它是一個視覺化參照，有助於將圖表物件與其代表的參數相關聯。 您可以使用圖註功能執行下列動作： • 將您的滑鼠指標移至圖註項目，以檢視它所代表的參數的更多資訊。 • 用滑鼠右鍵按一下圖註項目，以對其進行進一步調查。 • 按一下圖註項目，以在圖表中隱藏它。 再按一下圖註項目，以顯示隱藏的項目。 您也可以按一下對應的圖形項目，以隱藏和顯示該項目。 • 如果要從圖表顯示中移除圖註，按一下**圖註**。 **註**：僅當您選取「前次間隔（自動重新整理）」或以上的時間範圍，以及要顯示的分組選項時，才會顯示圖表。 **註**：如果您使用 Mozilla Firefox 作爲瀏覽器，並安裝了廣告封鎖程式瀏覽器延伸，則不顯示圖表。若要顯示圖表，則必須移除廣告封鎖程式瀏覽器延伸。如需相關資訊，請參閱瀏覽器說明文件。
來源 IP（唯一計數）	指定與此事件相關聯的來源 IP 位址。 如果有多個 IP 位址與此事件相關聯，則此欄位指定術語「多個」，以及 IP 位址的數目。

表 20. 分組事件參數 (繼續)

參數	說明
目的地 IP（唯一計數）	指定與此事件相關聯的目的地 IP 位址。 如果有多個 IP 位址與此事件相關聯，則此欄位指定術語「多個」，以及 IP 位址的數目。
目的地埠（唯一計數）	指定與此事件相關聯的目的地埠。 如果有多個埠與此事件相關聯，則此欄位指定術語「多個」，以及埠的數目。
事件名稱	指定事件的正規化名稱。
日誌來源（唯一計數）	指定將事件傳送給 QRadar 的日誌來源。如果有多個日誌來源與此事件相關聯，則此欄位指定術語「多個」，以及日誌來源的數目。
高階種類（唯一計數）	指定此事件的高階種類。 如果有多個種類與此事件相關聯，則此欄位指定術語「多個」，以及種類的數目。 如需種類的相關資訊，請參閱 *IBM Security QRadar Log Manager 管理手冊*。
低階種類（唯一計數）	指定此事件的低階種類。 如果有多個種類與此事件相關聯，則此欄位指定術語「多個」，以及種類的數目。
通訊協定（唯一計數）	指定與此事件相關聯的通訊協定 ID。 如果有多個通訊協定與此事件相關聯，則此欄位指定術語「多個」，以及通訊協定的數目。
使用者名稱（唯一計數）	指定與此事件相關聯的使用者名稱（若有）。如果有多個使用者名稱與此事件相關聯，則此欄位指定術語「多個」，以及使用者名稱的數目。
長度（上限）	指定計算的分組事件長度上限。 用來計算長度的變數包括可靠性、相關性與嚴重性。 如需可靠性、相關性與嚴重性的相關資訊，請參閱名詞解釋。
事件計數（總和）	指定此正規化事件中處理的事件總數。 若在短時間內偵測到相同來源及目的地 IP 位址有多個相同類型的事件，則會將這些事件組合起來。
計數	指定此事件群組中正規化事件的總數。

程序

1. 按一下**日誌活動**標籤。
2. 從**檢視**清單框中，選取要顯示的時間範圍。
3. 從「顯示」清單框中，選擇要作爲事件分組依據的參數。 請參閱表 2。列出事件群組。如需事件群組的詳細資料。 請參閱表 1。
4. 若要檢視某個群組的「事件清單」頁面，按兩下要調查的事件群組。 「事件清單」頁面不保留您在**日誌活動**標籤上所定義的圖表配置。如需「事件清單」頁面參數的相關資訊，請參閱表 1。
5. 若要檢視事件的詳細資料，按兩下要調查的事件。 如需事件的詳細資料，請參閱表 2。

事件詳細資料

您可以在各種模式下（包括串流模式）或在事件群組中檢視事件清單。 無論在您選擇檢視事件的何種模式下，您都可以尋找及檢視單一事件的詳細資料。

事件詳細資料頁面提供下列資訊：

表 21. 事件詳細資料

參數	**說明**
事件名稱	指定事件的正規化名稱。
低階種類	指定此事件的低階種類。 如需種類的相關資訊，請參閱 *IBM Security QRadar SIEM Administration Guide*。
事件說明	指定事件的說明（如果可用）。
長度	指定此事件的長度。 如需長度的相關資訊，請參閱名詞解釋
關聯	指定此事件的關聯。 如需關聯的相關資訊，請參閱名詞解釋。
嚴重性	指定此事件的嚴重性。 如需嚴重性的相關資訊，請參閱名詞解釋。
可靠性	指定此事件的可靠性。 如需可靠性的相關資訊，請參閱名詞解釋。
使用者名稱	指定與此事件相關聯的使用者名稱（如果可用）。
開始時間	指定從日誌來源接收事件的時間。
儲存時間	指定事件儲存在 QRadar 資料庫中的時間。
日誌來源時間	指定事件有效負載中日誌來源報告的系統時間。
異常偵測資訊 - 只有在異常偵測規則產生此事件時，才會顯示此窗格。 按一下**異常**圖示，可檢視導致異常偵測規則產生此事件的已儲存搜尋結果。	
規則說明	指定產生此事件的異常偵測規則。
異常說明	指定異常偵測規則偵測到的異常行爲的說明。
異常警示值	指定異常警示值。
來源及目的地資訊	
來源 IP	指定事件的來源 IP 位址。
目的地 IP	指定事件的目的地 IP 位址。
來源資產名稱	指定事件來源的使用者定義資產名稱。如需資產的相關資訊，請參閱「資產管理」。
目的地資產名稱	指定事件目的地的使用者定義資產名稱。如需資產的相關資訊，請參閱「資產管理」
來源埠	指定此事件的來源埠。
目的地埠	指定此事件的目的地埠。
前置 NAT 來源 IP	對於具有「網址轉換 (NAT)」功能的防火牆或其他裝置，此參數會在套用 NAT 值之前指定來源 IP 位址。NAT 可將一個網路中的 IP 位址轉換爲其他網路中的不同 IP 位址。

表 21. 事件詳細資料 (繼續)

參數	說明
前置 NAT 目的地 IP	對於具有 NAT 功能的防火牆或其他裝置，此參數會在套用 NAT 值之前指定目的地 IP 位址。
前置 NAT 來源埠	對於具有 NAT 功能的防火牆或其他裝置，此參數會在套用 NAT 值之前指定來源埠。
前置 NAT 目的地埠	對於具有 NAT 功能的防火牆或其他裝置，此參數會在套用 NAT 值之前指定目的地埠。
後置 NAT 來源 IP	對於具有 NAT 功能的防火牆或其他裝置，此參數會在套用 NAT 值之後指定來源 IP 位址。
後置 NAT 目的地 IP	對於具有 NAT 功能的防火牆或其他裝置，此參數會在套用 NAT 值之後指定目的地 IP 位址。
後置 NAT 來源埠	對於具有 NAT 功能的防火牆或其他裝置，此參數會在套用 NAT 值之後指定來源埠。
後置 NAT 目的地埠	對於具有 NAT 功能的防火牆或其他裝置，此參數會在套用 NAT 值之後指定目的地埠。
後置 NAT 來源埠	對於具有 NAT 功能的防火牆或其他裝置，此參數會在套用 NAT 值之後指定來源埠。
後置 NAT 目的地埠	對於具有 NAT 功能的防火牆或其他裝置，此參數會在套用 NAT 值之後指定目的地埠。
IPv6 來源	指定事件的來源 IPv6 位址。
IPv6 目的地	指定事件的目的地 IPv6 位址。
來源 MAC	指定事件的來源 MAC 位址。
目的地 MAC	指定事件的目的地 MAC 位址。
有效負載資訊	
有效負載	指定事件中的有效負載內容。此欄位提供 3 個標籤來檢視有效負載： • 通用傳輸格式 (UTF) - 按一下 UTF。 • 十六進位 - 按一下「十六進位」。 • Base64 - 按一下 Base64。
其他資訊	
通訊協定	指定與此事件相關聯的通訊協定。
QID	指定此事件的 QID。 每個事件都具有唯一的 QID。 如需對映 QID 的相關資訊，請參閱修改事件對映。
日誌來源	指定將事件傳送至 QRadar 的日誌來源。如果有多個與此事件相關聯的日誌來源，則此欄位會指定術語「多個」及日誌來源數目。
事件計數	指定組合在此正規化事件中的事件總數。 若在短時間內偵測到相同來源及目的地 IP 位址有多個相同類型的事件，則會將這些事件組合起來。
自訂規則	指定與此事件相符的自訂規則。 .
自訂規則部分符合	指定與此事件部分相符的自訂規則。

表 21. 事件詳細資料 (繼續)

參數	說明
註釋	指定此事件的註釋。 註釋是規則可以自動新增至事件的文字說明（作爲規則回應的一部分新增）。
識別資訊 - QRadar 會從日誌來源訊息收集識別資訊（如果可用）。 識別資訊提供了有關網路上資產的額外詳細資料。 只有當傳送至 QRadar 的日誌訊息包含 IP 位址及「使用者名稱」或「MAC 位址」項目時，日誌來源才會產生識別資訊。並非所有日誌來源都會產生識別資訊。 如需身分及資產的相關資訊，請參閱資產管理。	
身分使用者名稱	指定與此事件相關聯的資產的使用者名稱。
身分 IP	指定與此事件相關聯的資產的 IP 位址。
身分 Net BIOS 名稱	指定與此事件相關聯的資產的「網路基本輸入/輸出系統 (Net Bios)」名稱。
身分延伸欄位	指定與此事件相關聯的資產的相關資訊。 此欄位的內容是使用者定義的文字，且視網路上可用於提供識別資訊的裝置而定。 範例包括：裝置的實體位置、相關原則、網路交換器及埠名。
具有身分（旗標）	如果 QRadar 已收集與此事件相關聯的資產的識別資訊，請指定 True。 如需傳送識別資訊的裝置的相關資訊，請參閱 *IBM Security QRadar DSM Configuration Guide*。
身分主機名稱	指定與此事件相關聯的資產的主機名稱。
身分 MAC	指定與此事件相關聯的資產的 MAC 位址。
身分群組名稱	指定與此事件相關聯的資產的群組名稱。

事件詳細資料工具列

事件詳細資料工具列提供了數個用於檢視事件詳細資料的功能。

事件詳細資料工具列提供了下列功能：

表 22. 事件詳細資料工具列

回到事件清單	按一下**回到事件清單**，可回到事件的清單。
攻擊	按一下**攻擊**，可顯示與事件相關聯的攻擊。
異常	按一下**異常**，可顯示導致異常偵測規則產生此事件的已儲存搜尋結果。 **註**：只有在異常偵測規則產生此事件時，才會顯示此圖示。
對映事件	按一下**對映事件**，可編輯事件對映。 如需相關資訊，請參閱修改事件對映。
誤判	按一下**誤判**，可調整 QRadar 以防止誤判事件產生攻擊。
擷取內容	按一下**擷取內容**，可從選取的事件建立自訂事件內容。

表 22. 事件詳細資料工具列 (繼續)

前一個	按一下**前一個**，可檢視事件清單中的前一個事件。
下一個	按**下一個**，可檢視事件清單中的下一個事件。
PCAP 資料	**註**：只有在 QRadar 主控台已配置爲與 Juniper JunOS Platform DSM 整合時，才會顯示此選項。 如需管理 PCAP 資料的相關資訊，請參閱管理 PCAP 資料。 • **檢視 PCAP 資訊** - 選取此選項可檢視 PCAP 資訊。 如需相關資訊，請參閱檢視 PCAP 資訊。 • **下載 PCAP 檔案** - 選取此選項可將 PCAP 檔案下載至桌面系統。 如需相關資訊，請參閱將 PCAP 檔案下載至桌面系統。
列印	按一下**列印**，可列印事件詳細資料。

檢視關聯的攻擊

從「日誌活動」標籤中，您可以檢視與事件相關聯的攻擊。

關於這項作業

如果事件符合某項規則，則可以在**攻擊**標籤上產生攻擊。

如需規則的相關資訊，請參閱 *IBM Security QRadar SIEM Administration Guide*。

當您從**日誌活動**標籤檢視攻擊時，如果 Magistrate 尚未將與所選事件相關聯的攻擊儲存到磁碟，或者已從資料庫清除了攻擊，則可能不會顯示攻擊。 如果發生此狀況，則系統會通知您。

程序

1. 按一下**日誌活動**標籤。
2. 選用項目。 如果您正在串流模式中檢視事件，請按一下**暫停**圖示以暫停串流。
3. 按一下您要調查之事件旁的**攻擊**圖示。
4. 檢視關聯的攻擊。

修改事件對映

您可以手動將正規化或未處理的事件對映至高階或低階種類（或 QID）。

開始之前

此手動動作用來將不明日誌來源事件對映到已知的 QRadar 事件，以便可以適當地分類及處理它們。

關於這項作業

爲了進行正規化，QRadar 會自動將事件從日誌來源對映到高階和低階種類。

如需事件種類的相關資訊，請參閱*IBM Security QRadar SIEM Administration Guide*。

如果從日誌來源接收到系統無法分類的事件，則該事件會被分類爲不明。會發生這些事件的原因有幾個，其中包括：

- **使用者定義事件** - 部分日誌來源（如 Snort）將可讓您建立使用者定義事件。
- **新事件或較舊事件** - 供應商日誌來源可能將其軟體更新爲維護版本，以支援 QRadar 可能不支援的新事件。

註：當高階種類是 SIM Audit，或是日誌來源類型爲「簡易物件存取通訊協定 (SOAP)」時，對事件停用了**對映事件**圖示。

程序

1. 按一下**日誌活動**標籤。
2. 選用項目。 如果您正在串流模式中檢視事件，請按一下**暫停**圖示以暫停串流。
3. 按兩下要對映的事件。
4. 按一下**對映事件**。
5. 如果您知道要對映至此事件的 QID，請在**輸入 QID** 欄位中鍵入 QID。
6. 如果您不知道要對映至此事件的 QID，則可以搜尋特定的 QID：
   a. 選擇下列其中一個選項：若要根據種類來搜尋 QID，請從「高階種類」清單框來選取高階種類。 若要根據種類來搜尋 QID，請從「低階種類」清單框來選取低階種類。 若要根據日誌來源類型來搜尋 QID，請從「日誌來源類型」清單框來選取日誌來源類型。 若要根據名稱來搜尋 QID，請在「QID/名稱」欄位中鍵入名稱。
   b. 按一下**搜尋**。
   c. 選取要與此事件相關聯的 **QID**。
7. 按一下**確定**。

調整誤判

使用「誤判調整」功能來避免誤判事件建立攻擊。

開始之前

您可以從「事件清單」或「事件詳細資料」頁面調整誤判事件。

關於這項作業

您可以從「事件清單」或「事件詳細資料」頁面調整誤判事件。

您必須具有適當的權限才能建立調整誤判的自訂規則。

如需角色的相關資訊，請參閱*IBM Security QRadar SIEM Administration Guide*。

如需誤判的相關資訊，請參閱名詞解釋。

程序

1. 按一下**日誌活動**標籤。
2. 選用項目。 如果您正在串流模式中檢視事件，請按一下**暫停**圖示以暫停串流。
3. 選取您要調整的事件。
4. 按一下**誤判**。
5. 在「誤判」視窗上的「事件/流程內容」窗格中，請選取下列一項：
   - 具有特定 <Event> QID 的事件/流程
   - 具有 <Event> 低階種類的任何事件/流程
   - 具有 <Event> 高階種類的任何事件/流程
6. 在「傳輸方向」窗格中，請選取下列一項：
   - <來源 IP 位址> 到 <目的地 IP 位址>
   - <來源 IP 位址> 到任何目的地
   - 任何來源到 <目的地 IP 位址>
   - 任何來源至任何目的地
7. 按一下**調整**。

PCAP 資料

如果您的 QRadar 主控台配置爲與 Juniper JunOS Platform DSM 整合，則您可以接收及處理 Packet Capture (PCAP)，且可以從 Juniper SRX-Series ServicesGateway 日誌來源儲存資料。

如需 Juniper JunOS Platform DSM 的相關資訊，請參閱 *IBM Security QRadar DSM Configuration Guide*。

顯示 PCAP 資料直欄

依預設，**PCAP 資料**直欄不會顯示在**日誌活動**標籤上。 建立搜尋準則時，您必須選取「直欄定義」窗格中的 **PCAP 資料**直欄。

開始之前

必須使用「PCAP Syslog 組合」通訊協定配置 Juniper SRX-Series Services Gateway 日誌來源，您才能在**日誌活動**標籤上顯示 PCAP 資料。 如需配置日誌來源通訊協定的相關資訊，請參閱 *管理日誌來源手冊*。

關於這項作業

在您執行包含 **PCAP 資料**直欄的搜尋時，如果 PCAP 資料可用於事件，圖示會顯示在搜尋結果的 **PCAP 資料**直欄中。 使用 **PCAP** 圖示，您可以檢視 PCAP 資料，或將 **PCAP** 檔案下載至桌面系統。

程序

1. 按一下**日誌活動**標籤。
2. 從**搜尋**清單框中，選取**新建搜尋**。
3. 選用項目。 若要搜尋具有 PCAP 資料的事件，請配置下列搜尋準則：
   a. 從第一個清單框中，選取 **PCAP 資料**。

b. 從第二個清單框中，選取**等於**。
c. 從第三個清單框中，選取 **True**。
d. 按一下**新增過濾器**。

4. 配置直欄定義以包含 **PCAP 資料**直欄：
a. 從「直欄定義」窗格的**可用的直欄**清單中，按一下 **PCAP 資料**。
b. 按一下底端圖示集上的**新增直欄**圖示，以將 **PCAP 資料**直欄移至**直欄**清單。
c. 選用項目。 按一下頂端圖示集上的**新增直欄**圖示，以將 **PCAP 資料**直欄移至**分組依據**清單。
5. 按一下**過濾器**。
6. 選用項目。 如果您正在串流模式中檢視事件，請按一下**暫停**圖示以暫停串流。
7. 按兩下您要調查的事件。

下一步

如需檢視及下載 PCAP 資料的相關資訊，請參閱下列小節：

- 檢視 PCAP 資訊
- 將 PCAP 檔案下載至桌面系統

檢視 PCAP 資訊

從 **PCAP 資料**工具列功能表中，您可以檢視 PCAP 檔中資料的可讀版本，或者將 PCAP 檔下載到您的桌面系統。

開始之前

您必須先執行或選取顯示 **PCAP 資料**欄的搜尋，然後才可以檢視 PCAP 資訊。

關於這項作業

必須先擷取 PCAP 檔案，以便顯示在使用者介面上，然後才能顯示 PCAP 資料。 如果下載過程需要更多時間，則會顯示「正在下載 PCAP 封包資訊」視窗。 在大部分情況下，下載過程是一個快速過程，不會顯示該視窗。

擷取檔案之後，蹦現視窗會提供 PCAP 檔案的可讀版本。 您可以讀取視窗上顯示的資訊，或將資訊下載到您的桌面系統。

程序

1. 對於您要調查的事件，選擇下列其中一個選項：
   - 選取事件，然後按一下 **PCAP** 圖示。
   - 用滑鼠右鍵按一下事件的 **PCAP** 圖示，並選取**其他選項 > 檢視 PCAP 資訊**。
   - 按兩下您要調查的事件，然後從事件明細工具列選取 **PCAP 資料 > 檢視 PCAP 資訊**。
2. 如果要將資訊下載到您的桌面系統，請選擇下列其中一個選項：
   - 按一下**下載 PCAP 檔案**，以下載將在外部應用程式中使用的原始 PCAP 檔案。
   - 按一下**下載 PCAP 文字**，以下載 .TXT 格式的 PCAP 資訊。
3. 選擇下列其中一個選項：
   - 如果要開啓檔案立即檢視，請選取**開啓工具**選項，然後從清單框選取應用程式。

- 如果要儲存清單，請選取**儲存檔案**選項。

4. 按一下**確定**。

將 PCAP 檔案下載至桌面系統

您可以將 PCAP 檔案下載至桌面系統以進行儲存或用於其他應用程式。

開始之前

您必須執行或選取搜尋以顯示「PCAP 資料」直欄，才能檢視 PCAP 資訊。 請參閱**顯示 PCAP 資料直欄**。

程序

1. 針對要調查的事件，選擇下列其中一個選項：
   - 選取事件，然後按一下 **PCAP** 圖示。
   - 用滑鼠右鍵按一下事件的 PCAP 圖示，然後選取**其他選項 > 下載 PCAP 檔案**。
   - 用滑鼠右鍵按一下要調查的事件，然後從事件詳細資料工具列選取 **PCAP 資料 > 下載 PCAP 檔案**。
2. 選擇下列其中一個選項：
   - 如果您要開啓檔案以立即檢視，請選取**開啓工具**選項，然後從清單框中選取應用程式。
   - 如果您要儲存清單，請選取**儲存檔案**選項。
3. 按一下**確定**。

匯出事件

您可以用「延伸標記語言 (XML)」或「逗點區隔值 (CSV)」格式匯出事件。

開始之前

匯出資料所需的時間長度視指定的參數數目而定。

程序

1. 按一下**日誌活動**標籤。
2. 選用項目。 如果您正在串流模式中檢視事件，請按一下**暫停**圖示以暫停串流。
3. 從**動作**清單框中，選取下列其中一個選項：
   - **匯出至 XML > 可見的直欄** - 選取此選項，可僅匯出在「日誌活動」標籤上顯示的直欄。 這是建議的選項。
   - **匯出至 XML > 完全匯出（全部直欄）** - 選取此選項可匯出所有事件參數。 完全匯出可能需要較長時間才能完成。
   - **匯出至 CSV > 可見的直欄** - 選取此選項，可僅匯出在「日誌活動」標籤上顯示的直欄。這是建議的選項。
   - **匯出至 CSV > 完全匯出（全部直欄）** - 選取此選項可匯出所有事件參數。 完全匯出可能需要較長時間才能完成。
4. 如果匯出正在進行時，您要回復活動，請按一下**完成時通知**。

結果

匯出完成時，您會收到有關匯出完成的通知。 如果您未選取**完成時通知**圖示，畫面上會顯示狀態視窗。

第 6 章 網路活動調查

您可以使用**網路活動**標籤來即時監視及調查網路活動（流程）或執行進階搜尋

網路標籤概觀

使用**網路活動**標籤，您可以即時監視及調查網路活動（流程），或執行進階搜尋。

您必須具有檢視**網路活動**標籤的許可權。

如需許可權及指派角色的相關資訊，請參閱 *IBM Security QRadar SIEM Administration Guide*。

選取**網路活動**標籤，以視覺方式即時監視及調查流程資料，或執行進階搜尋以過濾顯示的流程。 流程是兩個主機之間的通訊階段作業。 您可以檢視流程資訊以判定資料流量的通訊方式，及通訊內容（如果已啓用內容擷取選項）。 流程資訊也可以包含通訊協定、「自主系統號碼 (ASN)」值或「介面索引 (IFIndex)」值之類的詳細資料。

網路活動標籤工具列

您可以從**網路活動**標籤工具列存取數個選項。

您可以從**網路活動**標籤工具列存取下列選項：

表 23. 網路活動標籤工具列選項

選項	說明
搜尋	按一下**搜尋**可對流程完成進階搜尋。 搜尋選項包括： • **新建搜尋** - 選取此選項可建立新的流程搜尋。 • **編輯搜尋** - 選取此選項可選取及編輯流程搜尋。 • **管理搜尋結果** - 選取此選項可檢視及管理搜尋結果。 如需搜尋功能的相關資訊，請參閱資料搜尋。
快速搜尋	從此清單框中，您可以執行先前儲存的搜尋。 僅當您具有已儲存的搜尋準則來指定**包含在我的快速搜尋中**選項時，選項才會顯示在**快速搜尋**清單框中。
新增過濾器	按一下**新增過濾器**，可將過濾器新增至現行搜尋結果。
儲存準則	按一下**儲存準則**可儲存現行搜尋準則。
儲存結果	按一下**儲存結果**可儲存現行搜尋結果。 此選項僅在搜尋完成之後顯示。 在串流模式下，此選項會停用。
取消	按一下**取消**可取消正在進行的搜尋。 在串流模式下，此選項會停用。

表 23. 網路活動標籤工具列選項 (繼續)

選項	說明
誤判	按一下**誤判**可開啓「誤判調整」視窗，以調除已知誤判的流程以防止建立攻擊。如需誤判的相關資訊，請參閱名詞解釋。 在串流模式下，此選項會停用。 請參閱匯出流程。
規則	僅在您具有檢視自訂規則的許可權時，才顯示**規則**選項。 選取下列其中一個選項： **規則** - 檢視或建立規則。 如果您具有檢視規則的許可權，畫面上會顯示「規則」精靈的摘要頁面。 如果您具有維護自訂規則的許可權，您可以編輯規則。 **註**：僅在您具有**網路活動 > 維護自訂規則**許可權時，才顯示異常偵測規則選項。 若要啓用異常偵測規則選項，您必須儲存聚集的搜尋準則。已儲存的搜尋準則指定必要的參數。 選取下列其中一個選項： **新增臨界值規則** - 建立臨界值規則。 臨界值規則可針對超出所配置臨界值的活動測試流程資料流量。 臨界值可以基於收集的任何資料。 例如，如果您建立臨界值規則，指出在 8 am 至 5 pm 之間登入伺服器的用戶端不能超過 220 個，則在第 221 個用戶端嘗試登入時，規則會產生警示。 **新增行為規則** - 建立行爲規則。 行爲規則測試一般週期性型樣發生的行爲中流量變更的流程資料流量。例如，如果郵件伺服器通常在午夜每秒與 100 個主機進行通訊，然後突然每秒開始與 1,000 個主機進行通訊，則行爲規則會產生警示。 **新增異常規則** - 建立異常規則。 異常規則可測試異常活動（如新的或不明資料流量）的流程資料流量。 例如，您可以建立異常規則，來將前 5 分鐘的平均資料流量與前一小時的平均資料流量比較。 如果變更超過 40%，規則會產生回應。 如需相關資訊，請參閱 *IBM Security QRadar SIEM Administration Guide*。

表 23. 網路活動標籤工具列選項 (繼續)

選項	說明
動作	按一下**動作**可完成下列動作： • **全部顯示** - 選取此選項可移除搜尋準則上的所有過濾器，及顯示所有未過濾的流程。 • **列印** - 選取此選項可列印頁面上顯示的流程。 • **匯出至 XML** - 選取此選項以 XML 格式匯出流程。 請參閱匯出流程。 • **匯出至 CSV** - 選取此選項以 CSV 格式匯出流程。 請參閱匯出流程。 • **刪除** - 選取此選項可刪除搜尋結果。 請參閱資料搜尋。 • **通知** - 選取此選項，可指定您要在完成選取的搜尋時獲得電子郵件通知。 此選項僅對正在進行的搜尋啓用。 **註**：在串流模式下及在檢視部分搜尋結果時，**列印**、**匯出至 XML** 及**匯出至 CSV** 選項會停用。
搜尋工具列	**進階搜尋** 從清單框中選取**進階搜尋**，然後輸入 Ariel 查詢語言 (AQL) 搜尋字串來指定要傳回的欄位。 **快速過濾器** 從清單框中選取**快速過濾器**，以透過使用簡式字詞或片語來搜尋有效負載。
視圖	**網路活動**標籤上的預設視圖是即時事件的串流。**視圖**清單包含一些選項，也可檢視指定時段中的事件。在從**視圖**清單中選擇指定的時段之後，您就可以變更**開始時間**及**結束時間**欄位中的日期和時間值，來修改顯示的時段。

右鍵功能表選項

在**網路活動**標籤上，您可以用滑鼠右鍵按一下流程以存取更多流程過濾器準則。

右鍵功能表選項爲：

表 24. 右鍵功能表選項

選項	說明
過濾	選取此選項可過濾選取的流程，具體視流程中選取的參數而定。
誤判	選取此選項可開啓「誤判調整」視窗，此視窗可讓您調除已知誤判的流程以防止建立攻擊。在串流模式下，此選項會停用。 請參閱匯出流程。
其他選項：	選取此選項可調查 IP 位址。請參閱調查 IP 位址。 **註**：在串流模式下，不會顯示此選項。

表 24. 右鍵功能表選項 (繼續)

選項	說明
快速過濾器	過濾符合或不符合選取項目的項目。

狀態列

串流流程時，狀態列會顯示每秒收到的平均結果數目。

這是主控台成功從事件處理器收到的結果數目。 如果每秒此數目超過 40 個結果，畫面上僅顯示 40 個結果。 餘數會累計在結果緩衝區中。 若要檢視更多狀態資訊，請將滑鼠指標移在狀態列上。

未串流流程時，狀態列顯示目前顯示的搜尋結果數目及處理搜尋結果所需的時間量。

溢位記錄

使用管理許可權，您可以指定要從 QRadar QFlow 收集器 傳送至事件處理器的流程數目上限。

如果具有管理許可權，您可以指定要從 QRadar QFlow 收集器 傳送至事件處理器的流程數目上限。 在達到配置的流程限制之後收集的所有資料都會分組成一個流程記錄。 然後，此流程記錄會顯示在**網路活動**標籤上，來源 IP 位址爲 127.0.0.4，目的地 IP 位址爲 127.0.0.5。 此流程記錄在**網路活動**標籤上指定溢位。

網路活動監視

依預設，**網路活動**標籤會在串流模式中顯示流程，以讓您即時檢視流程。

如需串流模式的相關資訊，請參閱檢視串流流程。 您可以使用**視圖**清單框指定不同的時間範圍來過濾流程。

如果您先前將已儲存的搜尋配置爲預設值，則存取**網路活動**標籤時，會自動顯示該搜尋的結果。 如需儲存搜尋準則的相關資訊，請參閱儲存事件及流程搜尋準則。

檢視串流流程

串流模式容許您檢視輸入系統的流程資料。 此模式爲您提供現行流程活動的即時視圖，顯示前 50 個流程。

關於這項作業

如果在啓用串流模式之前，您在「網路活動」標籤上或搜尋準則中套用了任何過濾器，則會以串流模式保留過濾器。 但是，串流模式不支援包括分組流程的搜尋。 如果對分組流程或分組搜尋準則啓用串流模式，則「網路活動」標籤會顯示正規化流程。 請參閱「檢視正規化流程」。

當您要選取流程以檢視詳細資料或執行動作時，必須先暫停串流，才能按兩下事件。 暫停串流時，會顯示前 1000 個流程。

程序

1. 按一下**網路活動**標籤。

2. 從「檢視」清單框中，選取**即時（串流）**。
如需工具列選項的相關資訊，請參閱表 5-1。 如需以串流模式顯示參數的相關資訊，請參閱表 5-3。
3. 選用項目。 暫停或播放串流流程。 選擇下列其中一個選項：
   - 若要選取事件記錄，請按一下**暫停**圖示以暫停串流。
   - 若要重新啓動串流模式，請按一下**播放**圖示。

檢視正規化流程

收集、正規化資料流程，然後將其顯示在**網路活動**標籤上。

關於這項作業

正規化涉及準備流程資料，以顯示可讀的標籤相關資訊。

註：如果選取要顯示的時間範圍，則會顯示時間序列圖表。 如需使用時間序列圖表的相關資訊，請參閱時間序列圖表概觀。

當您檢視正規化流程時，**網路活動**標籤顯示下列參數：

表 25. 「網路活動」標籤的參數

參數	說明
現行過濾器	此表格頂端顯示套用到搜尋結果的過濾器的詳細資料。 若要清除這些過濾器值，請按一下**清除過濾器**。 **註**：僅當套用過濾器之後才會顯示這個參數。
檢視	從這個清單框中，您可以選取要過濾的時間範圍。
現行統計資料	當未使用「即時（串流）」或「前一分鐘（自動重新整理）」模式時，會顯示現行統計資料，包括： **註**：按一下「現行統計資料」旁的箭頭，以顯示或隱藏統計資料。 • **結果總計** - 指定符合搜尋準則的結果總數。 • **已搜尋的資料檔案** - 指定在指定期間跨距內已搜尋的資料檔案總數。 • **已搜尋的壓縮資料檔案** - 指定在指定期間跨距內已搜尋的壓縮資料檔案總數。 • **索引檔案計數** - 指定在指定期間跨距內已搜尋的索引檔案總數。 • **持續時間** - 指定搜尋的持續時間。 **註**：現行統計資料有助於進行疑難排解。 當您聯絡客戶支援中心，以對流程進行疑難排解時，可能會被要求提供現行統計資訊。

表 25. 「網路活動」標籤的參數 (繼續)

參數	說明
圖表	顯示可配置圖表，以代表符合時間間隔與分組選項的記錄。 如果要從顯示畫面中移除圖表，按一下**隱藏圖表**。 僅當您選取「前次間隔（自動重新整理）」或以上的時間範圍，以及要顯示的分組選項時，才會顯示圖表。 如需配置圖表的相關資訊，請參閱配置圖表。 **註**：如果您使用 Mozilla Firefox 作爲瀏覽器，並安裝了廣告封鎖程式瀏覽器延伸，則不顯示圖表。 若要顯示圖表，則必須移除廣告封鎖程式瀏覽器延伸。 如需相關資訊，請參閱瀏覽器說明文件。
攻擊圖示	按一下**攻擊**圖示，以檢視與此流程相關聯的攻擊的詳細資料。
流程類型	指定流程類型。 流程類型可透過送入活動與送出活動的比例來測量。 流程類型包括： • **標準流程** - 雙向傳輸 • **A 類** - 單對多（單向），例如，執行網路掃描的單個主機。 • **B 類** - 多對單（單向），例如，分佈式 DoS (DDoS) 攻擊。 • **C 類** - 單對單（單向），例如，主機到主機埠掃描。
第一次封包時間	指定接收流程的日期和時間。
儲存時間	指定將流程儲存在 QRadar 資料庫中的時間。
來源 IP	指定流程的來源 IP 位址。
來源埠	指定流程的來源埠。
目的地 IP	指定流程的目的地 IP 位址。
目的地埠	指定流程的目的地埠。
來源位元組數	指定從來源主機傳送的位元組數。
目的地位元組數	指定從目的地主機傳送的位元組數。
位元組總數	指定與流程相關聯的位元組總數。
來源封包	指定從來源主機傳送的封包總數。
目的地封包	指定從目的地主機傳送的封包總數。
封包總數	指定與流程相關聯的封包總數。
通訊協定	指定與流程相關聯的通訊協定。
應用程式	指定偵測到的流程應用程式。 如需應用程式偵測的相關資訊，請參閱 *IBM Security QRadar 應用程式配置手冊*。

表 25. 「網路活動」標籤的參數 (繼續)

參數	說明
ICMP 類型/代碼	指定「網際網路控制訊息通訊協定 (ICMP)」類型與編碼（若有）。 如果流程具有已知格式的 ICMP 類型與編碼資訊，則此欄位顯示爲「<A> 類」。 編碼 <B>，其中 <A> 與 <B> 是類型與編碼的數值。
來源旗標	指定來源封包中偵測到的「傳輸控制通訊協定 (TCP)」旗標（若有）。
目的地旗標	指定目的地封包中偵測到的 TCP 旗標（若有）。
來源服務品質	指定流程的「服務品質 (QoS)」服務等級。 QoS 讓網路能夠提供各種流程服務層次。 QoS 提供下列基本服務等級： • **最佳效能** - 此服務等級不保證遞送。 遞送流程被認爲是最佳效能。 • **分級式服務** - 授予特定流程高於其他流程的優先順序。 依資料流量分類授予此優先順序。 • **保證服務** - 此服務等級保證爲特定流程預約網路資源。
目的地服務品質	指定目的地流程的服務品質服務層次。
流程來源	指定偵測到流程的系統。
流程介面	指定接收流程的介面。
來源 IFIndex	指定來源「介面索引 (IFIndex)」號碼。
目的地 IFIndex	指定目的地 IFIndex 號碼。
來源 ASN	指定來源「自主系統號碼 (ASN)」值。
目的地 ASN	指定目的地 ASN 值。

程序

1. 按一下**網路活動**標籤。
2. 從**顯示**清單框中，選取**預設（正規化）**。
3. 從**檢視**清單框中，選取要顯示的時間範圍。
4. 按一下**暫停**圖示，以暫停串流。
5. 按兩下要進一步檢視明細的流程。 請參閱流程明細。

檢視分組流程

您可以使用**網路活動**標籤，檢視依各種選項分組的流程。 從**顯示**清單框中，可以選取作爲流程分組依據的參數。

關於這項作業

顯示清單框不會以串流模式顯示，因爲串流模式不支援分組流程。 如果使用未分組的搜尋準則進入串流模式，則會顯示此選項。

顯示清單框提供下列選項：

表 26. 分組流程選項

分組選項	**說明**
來源或目的地 IP	顯示依流程關聯的 IP 位址分組的流程彙總清單。
來源 IP	顯示依流程的來源 IP 位址分組的流程彙總清單。
目的地 IP	顯示依流程的目的地 IP 位址分組的流程彙總清單。
來源埠	顯示依流程的來源埠分組的流程彙總清單。
目的地埠	顯示依流程的目的地埠分組的流程彙總清單。
來源網路	顯示依流程的來源網路分組的流程彙總清單。
目的地網路	顯示依流程的目的地網路分組的流程彙總清單。
應用程式	顯示依流程的來源應用程式分組的流程彙總清單。
地理	顯示依地理位置分組的流程彙總清單。
通訊協定	顯示依流程關聯的通訊協定分組的流程彙總清單。
流程偏移	顯示依流程方向分組的流程彙總清單。
ICMP 類型	顯示依流程的 ICMP 類型分組的流程彙總清單。

從**顯示**清單框選取選項之後，資料的直欄佈置視所選群組選項而定。流程表格中的每一列代表一個流程群組。 **網路活動**標籤提供每一個流程群組的下列資訊。

表 27. 分組流程參數

標頭	**說明**
分組依據	指定作爲搜尋分組依據的參數。
現行過濾器	此表格頂端顯示套用到搜尋結果的過濾器的詳細資料。 若要清除這些過濾器值，請按一下**清除過濾器**。
檢視	從清單框中，選取要過濾的時間範圍。

表 27. 分組流程參數 (繼續)

標頭	說明
現行統計資料	當未使用「即時（串流）」或「前一分鐘（自動重新整理）」模式時，會顯示現行統計資料，包括： **註**：按一下**現行統計資料**旁的箭頭，以顯示或隱藏統計資料。 • **結果總計** - 指定符合搜尋準則的結果總數。 • **已搜尋的資料檔案** - 指定在指定期間跨距內已搜尋的資料檔案總數。 • **已搜尋的壓縮資料檔案** - 指定在指定期間跨距內已搜尋的壓縮資料檔案總數。 • **索引檔案計數** - 指定在指定期間跨距內已搜尋的索引檔案總數。 • **持續時間** - 指定搜尋的持續時間。 **註**：現行統計資料有助於進行疑難排解。 當您聯絡客戶支援中心，以對流程進行疑難排解時，可能會被要求提供現行統計資訊。
圖表	顯示可配置圖表，以代表符合時間間隔與分組選項的記錄。如果要從顯示畫面中移除圖表，按一下**隱藏圖表**。 僅當您選取「前次間隔（自動重新整理）」或以上的時間範圍，以及要顯示的分組選項時，才會顯示圖表。 如需配置圖表的相關資訊，請參閱配置圖表。 **註**：如果您使用 Mozilla Firefox 作爲瀏覽器，並安裝了廣告封鎖程式瀏覽器延伸，則不顯示圖表。若要顯示圖表，則必須移除廣告封鎖程式瀏覽器延伸。如需相關資訊，請參閱瀏覽器說明文件。
來源 IP（唯一計數）	指定流程的來源 IP 位址。
目的地 IP（唯一計數）	指定流程的目的地 IP 位址。 如果有多個目的地 IP 位址與此流程相關聯，則此欄位指定術語「多個」，以及 IP 位址的數目。
來源埠（唯一計數）	顯示流程的來源埠。
目的地埠（唯一計數）	指定流程的目的地埠。如果有多個目的地埠與此流程相關聯，則此欄位指定術語「多個」，以及埠的數目。
來源網路（唯一計數）	指定流程的來源網路。 如果有多個來源網路與此流程相關聯，則此欄位指定術語「多個」，以及網路的數目。
目的地網路（唯一計數）	指定流程的目的地網路。如果有多個目的地網路與此流程相關聯，則此欄位指定術語「多個」，以及網路的數目。
應用程式（唯一計數）	指定偵測到的流程應用程式。如果有多個應用程式與此流程相關聯，則此欄位指定術語「多個」，以及應用程式的數目。

表 27. 分組流程參數 (繼續)

標頭	說明
來源位元組（總和）	指定從來源傳送的位元組數。
目的地位元組（總和）	指定從目的地傳送的位元組數。
位元組總數（總和）	指定與流程相關聯的位元組總數。
來源封包（總和）	指定從來源傳送的封包數。
來源封包（總和）	指定從來源傳送的封包數。
來源封包（總和）	指定從來源傳送的封包數。
目的地封包（總和）	指定從目的地傳送的封包數。
封包總數（總和）	指定與流程相關聯的封包總數。
計數	指定傳送或接收的流程數。

程序

1. 按一下**網路活動**標籤。
2. 從**檢視**清單框中，選取要顯示的時間範圍。
3. 從**顯示**清單框中，選擇要作爲流程分組依據的參數。 請參閱表 2。 列出流程群組。 如需流程群組的詳細資料。 請參閱表 1。
4. 若要檢視某個群組的「流程清單」頁面，按兩下要調查的流程群組。 「流程清單」頁面不保留您在**網路活動**標籤上所定義的圖表配置。 如需「流程清單」參數的相關資訊，請參閱表 2。
5. 若要檢視流程的詳細資料，按兩下要調查的流程。 如需流程明細頁面的相關資訊，請參閱表 1。

流程詳細資料

您可以在各種模式下（包括串流模式）或在流程群組中檢視流程清單。 無論在您選擇檢視流程的何種模式下，您都可以尋找及檢視單一流程的詳細資料。

流程詳細資料頁面提供下列資訊：

表 28. 流程詳細資料

參數	說明
流程資訊	
通訊協定	指定與此流程相關聯的通訊協定。 如需通訊協定的相關資訊，請參閱 *IBM Security QRadar 應用程式配置手冊*。
應用程式	指定流程之偵測到的應用程式。如需應用程式偵測的相關資訊，請參閱 *IBM Security QRadar 應用程式配置手冊*。
長度	指定此流程的長度。如需長度的相關資訊，請參閱名詞解釋。
關聯	指定此流程的關聯。如需關聯的相關資訊，請參閱名詞解釋。
嚴重性	指定此流程的嚴重性。如需嚴重性的相關資訊，請參閱名詞解釋。

表 28. 流程詳細資料 (繼續)

參數	說明
可靠性	指定此流程的可靠性。如需可靠性的相關資訊，請參閱名詞解釋。
第一次封包時間	指定流程來源報告的流程的開始時間。 如需流程來源的相關資訊，請參閱 *IBM Security QRadar SIEM Administration Guide*。
最後一次封包時間	指定流程來源報告的流程的結束時間。
儲存時間	指定流程儲存在 QRadar 資料庫中的時間。
事件名稱	指定流程的正規化名稱。
低階種類	指定此流程的低階種類。 如需種類的相關資訊，請參閱 *IBM Security QRadar SIEM Administration Guide*。
事件說明	指定流程的說明（如果可用）。
來源及目的地資訊	
來源 IP	指定流程的來源 IP 位址。
目的地 IP	指定流程的目的地 IP 位址。
來源資產名稱	指定流程的來源資產名稱。如需資產的相關資訊，請參閱資產管理。
目的地資產名稱	指定流程的目的地資產名稱。 如需資產的相關資訊，請參閱資產管理。
IPv6 來源	指定流程的來源 IPv6 位址。
IPv6 目的地	指定流程的目的地 IPv6 位址。
來源埠	指定流程的來源埠。
目的地埠	指定流程的目的地埠。
來源服務品質	指定來源流程的服務的服務品質層次。
目的地服務品質	指定目的地流程的服務的服務品質層次。
來源 ASN	指定來源 ASN 號碼。 **註**：如果此流程具有來自多個流程來源的重複記錄，則會列出對應的來源 ASN 號碼。
目的地 ASN	指定目的地 ASN 號碼。 **註**：如果此流程具有來自多個流程來源的重複記錄，則會列出對應的目的地 ASN 號碼。
來源 IFIndex	指定來源 IFIndex 號碼。 **註**：如果此流程具有來自多個流程來源的重複記錄，則會列出對應的來源 IFIndex 號碼。
目的地 IFIndex	指定目的地 IFIndex 號碼。 **註**：如果此流程具有來自多個流程來源的重複記錄，則會列出對應的目的地 IFIndex 號碼。
來源有效負載	指定來源有效負載的封包及位元組計數。
目的地有效負載	指定目的地有效負載的封包及位元組計數。
有效負載資訊	

表 28. 流程詳細資料 (繼續)

參數	說明
來源有效負載	指定流程中的來源有效負載內容。此欄位提供 3 種格式來檢視有效負載： • 通用傳輸格式 (UTF) - 按一下 UTF。 • 十六進位 - 按一下「十六進位」。 • Base64 - 按一下 Base64。 **註**：如果您的流程來源是 Netflow 第 9 版或 IPFIX，來自這些來源的未剖析欄位可能會顯示在**來源有效負載**欄位中。 未剖析欄位的格式爲 <name>=<value>。 例如，MN_TTL=x
目的地有效負載	指定流程中的目的地有效負載內容。 此欄位提供 3 種格式來檢視有效負載： • 通用傳輸格式 (UTF) - 按一下 **UTF**。 • 十六進位 - 按一下**十六進位**。 • Base64 - 按一下 **Base64**。
其他資訊	
流程類型	指定流程類型。 流程類型可透過送入活動與送出活動的比例來測量。流程類型包括： • 標準 - 雙向資料流量 • 類型 A - 一對多（單向） • 類型 B - 多對一（單向） • 類型 C - 一對一（單向）
流程方向	指定流程的方向。 流程方向包括： • L2L - 從某個本端網路至另一個本端網路的內部資料流量。 • L2R - 從本端網路至遠端網路的內部資料流量。 • R2L - 從遠端網路至本端網路的內部資料流量。 • R2R - 從某個遠端網路至另一個遠端網路的內部資料流量。
自訂規則	指定與此流程相符的自訂規則。 如需規則的相關資訊，請參閱 *IBM Security QRadar SIEM Administration Guide*。
自訂規則部分符合	指定與此流程部分相符的自訂規則。
流程來源/介面	指定偵測到流程的系統的流程來源名稱。 **註**：如果此流程具有來自多個流程來源的重複記錄，則會列出對應的流程來源。
註釋	指定此流程的註釋或附註。註釋是規則可以自動新增至流程的文字說明（作爲規則回應的一部分新增）。

流程詳細資料工具列

流程詳細資料工具列提供各種功能。

流程詳細資料工具列提供下列功能

表 29. 流程詳細資料工具列的說明

功能	說明
回到結果	按一下**回到結果**，可回到流程清單。
擷取內容	按一下**擷取內容**，可從選取的流程建立自訂流程內容。 如需相關資訊，請參閱「自訂事件及流程內容」。
誤判	按一下**誤判**，可開啓「誤判調整」視窗，此視窗可讓您調除已知誤判的流程以防止建立攻擊。 在串流模式下，此選項會停用。請參閱匯出流程。
前一個	按一下**前一個**，可檢視流程清單中的前一個流程。
下一個	按**下一個**，可檢視流程清單中的下一個流程。
列印	按一下**列印**，可列印流程詳細資料。
攻擊	如果**攻擊**可用，請按一下以檢視「攻擊摘要」頁面。

調整誤判

使用「誤判調整」功能來避免誤判流程建立攻擊。 您可以從流程清單或流程詳細資料頁面調整誤判流程。

關於這項作業

註：您可以從摘要或詳細資料頁面調整誤判流程。

您必須具有適當的權限才能建立調整誤判的自訂規則。 如需誤判的相關資訊，請參閱名詞解釋。

程序

1. 按一下**網路活動**標籤。
2. 選用項目。 如果您正在串流模式中檢視流程，請按一下**暫停**圖示以暫停串流。
3. 選取您要調整的流程。
4. 按一下**誤判**。
5. 在「誤判」視窗上的「事件/流程內容」窗格中，請選取下列一項：
   - 具有特定 <Event> QID 的事件/流程
   - 具有 <Event> 低階種類的任何事件/流程
   - 具有 <Event> 高階種類的任何事件/流程
6. 在「傳輸方向」窗格中，請選取下列一項：
   - <來源 IP 位址> 到 <目的地 IP 位址>
   - <來源 IP 位址> 到任何目的地

- 任何來源到 <目的地 IP 位址>
- 任何來源至任何目的地

7. 按一下**調整**。

匯出流程

您可以用「延伸標記語言 (XML)」或「逗點區隔值 (CSV)」格式匯出流程。 匯出資料所需的時間長度視指定的參數數目而定。

程序

1. 按一下**網路活動**標籤。
2. 選用項目。 如果您正在串流模式中檢視流程，請按一下**暫停**圖示以暫停串流。
3. 從**動作**清單框中，選取下列其中一個選項：
   - **匯出至 XML > 可見的直欄** - 選取此選項，可僅匯出在「日誌活動」標籤上顯示的直欄。 這是建議的選項。
   - **匯出至 XML > 完全匯出（全部直欄）** - 選取此選項可匯出所有流程參數。 完全匯出可能需要較長時間才能完成。
   - **匯出至 CSV > 可見的直欄** - 選取此選項，可僅匯出在「日誌活動」標籤上顯示的直欄。 這是建議的選項。
   - **匯出至 CSV > 完全匯出（全部直欄）** - 選取此選項可匯出所有流程參數。 完全匯出可能需要較長時間才能完成。
4. 如果您要回復活動，請按一下**完成時通知**。

結果

匯出完成時，您會收到有關匯出完成的通知。 如果您未選取**完成時通知**圖示，畫面上會顯示狀態視窗。

第 7 章 資產管理

收集及檢視資產資料可幫助您識別威脅和漏洞。 精確的資產資料庫可讓您更輕易將在您系統中所觸發的攻擊連接至您網路中的實體或虛擬資產。

限制：QRadar Log Manager 僅在安裝了 QRadar Vulnerability Manager 時追蹤資產資料。如需 IBM Security QRadar SIEM 與 IBM Security QRadar Log Manager 之間差異的相關資訊，請參閱第 5 頁的『安全智慧產品中的功能』。

資產資料

資產 (asset) 是指任何透過您的網路基礎架構傳送或接收資料的網路端點。例如，筆記型電腦、伺服器、虛擬機器和手提式裝置全部都是資產。 資產資料庫中的每個資產都會獲指派一個唯一 ID，以便與其他資產記錄區別。

偵測裝置對於建置關於資產的歷程資訊資料集也非常有用。 隨資產資訊變更而追蹤它可幫助您監視在您的網路中的資產使用情形。

資產設定檔

資產設定檔 (asset profile) 是指 IBM Security QRadar SIEM 在一段時間內收集關於特定資產之所有資訊的集合。 此設定檔包含在資產上執行之服務的相關資訊以及所顯示的任何身分資訊。

QRadar SIEM 會自動從身分事件以及雙向流程資料或漏洞評量掃描（如果已配置的話）建立資產設定檔。 系統會透過稱爲*資產核對 (asset reconciliation)* 的程序使資料產生關聯，並在新資訊進入 QRadar 時更新設定檔。系統會按照下列優先順序，從資產更新項目中的資訊衍生資產名稱：

- 給定名稱
- NETBios 主機名稱
- DNS 主機名稱
- IP 位址

收集資產資料

資產設定檔根據識別資訊動態建置，而識別資訊是從事件或流程資料或在漏洞掃描期間 QRadar 主動尋找的資料被動吸收的。您也可以匯入資產資料，或手動編輯資產設定檔。

資產資料的來源

資產資料是從您的 IBM Security QRadar 部署中的數個不同來源所接收。

資產資料會以漸進方式寫入資產資料庫，通常一次爲兩項或三項資料。 除了來自網路漏洞掃描器的更新項目例外之外，每一個資產更新項目一次僅包含一個資產的相關資訊。

資產資料通常來自下列其中一個資產資料來源：

事件 事件有效負載（如 DHCP 或鑑別伺服器所建立的內容）經常包含使用者登入、IP 位址、主機名稱、MAC 位址，以及其他資產資訊。 這項資料會立即提供給資產資料庫，以幫助確定資產更新項目套用到哪一個資產。

事件是資產成長偏差的主要原因。

流程 流程有效負載包含通訊資訊，如 IP 位址、埠，以及在一般、可配置間隔內所收集的通訊協定。在每一個間隔結尾，會將資料提供給資產資料庫，一次一個 IP 位址。

由於來自流程的資產資料會根據單一 ID、IP 位址與資產配對，因此流程資料從來不會是資產成長偏差的原因。

漏洞掃描器

QRadar 同時與 IBM 和協力廠商漏洞掃描器整合，可提供作業系統、已安裝軟體和修補程式資訊之類的資產資料。 該資料的類型會隨掃描器而異，並可能隨掃描而異。 在探索到新資產、埠資訊和漏洞時，系統會根據掃描中所定義的 CIDR 範圍，將資料送入資產設定檔中。

掃描器有可能會引入資產成長偏差，但是並不常見。

使用者介面

具有「資產」角色的使用者可以將資產資訊直接匯入或提供到資產資料庫。 使用者所直接提供的資產更新項目是用於特定的資產，因此會略過資產核對階段。

使用者所提供的資產更新項目不會引入資產成長偏差。

網域察覺資產資料

以網域資訊配置了資產資料來源時，所有來自該資料來源的資產資料都會自動標示相同的網域。 由於資產模型中的資料爲網域察覺，因此網域資訊會套用到所有 QRadar 元件，其中包括身分、攻擊、資產設定檔和伺服器探索。

當您檢視資產設定檔時，某些欄位可能是空白的。 當系統未接收資產更新項目中的這項資訊，或是資訊已超出資產保留期時，就會存在空白欄位。 預設保留期爲 120 天。 顯示爲 0.0.0.0 的 IP 位址表示資產不包含 IP 位址資訊。

送入的資產資料的工作流程

此工作流程說明 QRadar 如何使用事件有效負載中的身分資訊來決定是要建立新資產還是更新現有的資產。

1. QRadar 接收事件。 資產側寫程式在事件有效負載中檢查身分資訊。
2. 如果身分資訊包含已經與資產資料庫中的資產相關聯的 MAC 位址、NetBIOS 主機名稱或 DNS 主機名稱，則會以所有新資訊更新該資產。
3. 如果唯一可用的身分資訊是 IP 位址，則系統會將更新項目與具有相同 IP 位址的現有資產核對。
4. 如果資產更新項目包含符合現有資產的 IP 位址，但是也包含更多不符合現有資產的身分資訊，則系統會在現有資產更新之前，使用其他資訊來排除誤判相符項。
5. 如果身分資訊不符合資料庫中的現有資產，則會根據事件有效負載中的資訊來建立新資產。

資產資料更新

IBM Security QRadar 使用事件有效負載中的身分資訊來決定是要建立新資產還是更新現有的資產。

每一個資產更新項目都必須包含關於單一資產的受信任資訊。 當 QRadar 接收資產更新項目時，系統會決定更新項目套用到哪個資產。

資產核對 (Asset reconciliation) 是確定資產更新項目與資產資料庫中相關資產之間的關係之處理程序。 資產核對發生於 QRadar 接收更新項目之後，但是在資訊寫入資產資料庫之前。

身分資訊

每個資產至少必須包含一份身分資料。 系統會將包含一或多份該相同身分資料的後續更新項目與擁有該資料的資產核對。 系統會小心處理根據 IP 位址的更新項目以避免誤判資產相符項。 將系統中的一個資產先前所擁有之 IP 位址的所有權指派給另一個實體資產時，會發生誤判資產相符項。

當提供了多份身分資料時，資產側寫程式會以下列順序設定資訊的優先順序：

- MAC MAC 位址（最具決定性的）
- NetBIOS 主機名稱
- DNS 主機名稱
- IP 位址（最不具決定性的）

MAC 位址、NetBIOS 主機名稱和 DNS 主機名稱必須是唯一的，也因此被視爲決定性的身分資料。 僅依 IP 位址符合現有資產的送入更新項目的處理方式，與符合更決定性身分資料的更新項目的處理方式不同。

相關概念:

『資產核對排除規則』
針對進入 IBM Security QRadar 的每一個資產項目，資產核對排除規則會將測試套用到資產更新項目中的 NetBIOS 主機名稱、DNS 主機名稱和 IP 位址。

資產核對排除規則

針對進入 IBM Security QRadar 的每一個資產項目，資產核對排除規則會將測試套用到資產更新項目中的 NetBIOS 主機名稱、DNS 主機名稱和 IP 位址。

依預設，系統會在兩小時期間內追蹤每一項資產資料。 如果資產更新項目中的任何一項身分資料在 2 小時內兩次以上顯出可疑的行爲，該資料項目就會新增至資產黑名單。 所測試的每一種類型的身分資產資料都有分開的黑名單。

在網域察覺環境中，資產核對排除規則會針對每一個網域分開追蹤資產資料的行爲。

資產核對排除規則會測試下列範例情節：

表 30. 規則測試與回應

範例情節	規則回應
當 MAC 位址在 2 小時或以內與三個以上的不同 IP 位址相關聯時	將 MAC 位址新增至資產核對網域 MAC 黑名單

表 30. 規則測試與回應 (繼續)

範例情節	規則回應
當 DNS 主機名稱在 2 小時或以內與三個以上的不同 IP 位址相關聯時	將 DNS 主機名稱新增至「資產核對網域 DNS」黑名單
當 NetBIOS 主機名稱在 2 小時或以內與三個以上的不同 IP 位址相關聯時	將 NetBIOS 主機名稱新增至「資產核對網域 NetBIOS」黑名單
當 IPv4 位址在 2 小時或以內與三個以上的不同 MAC 位址相關聯時	將 IP 位址新增至「資產核對網域 IPv4」黑名單
當 NetBIOS 主機名稱在 2 小時或以內與三個以上的不同 MAC 位址相關聯時	將 NetBIOS 主機名稱新增至「資產核對網域 NetBIOS」黑名單
當 DNS 主機名稱在 2 小時或以內與三個以上的不同 MAC 位址相關聯時	將 DNS 主機名稱新增至「資產核對網域 DNS」黑名單
當 IPv4 位址在 2 小時或以內與三個以上的不同 DNS 主機名稱相關聯時	將 IP 位址新增至「資產核對網域 IPv4」黑名單
當 NetBIOS 主機名稱在 2 小時或以內與三個以上的不同 DNS 主機名稱相關聯時	將 NetBIOS 主機名稱新增至「資產核對網域 NetBIOS」黑名單
當 MAC 位址在 2 小時或以內與三個以上的不同 DNS 主機名稱相關聯時	將 MAC 位址新增至資產核對網域 MAC 黑名單
當 IPv4 位址在 2 小時或以內與三個以上的不同 NetBIOS 主機名稱相關聯時	將 IP 位址新增至「資產核對網域 IPv4」黑名單
當 DNS 主機名稱在 2 小時或以內與三個以上的不同 NetBIOS 主機名稱相關聯時	將 DNS 主機名稱新增至「資產核對網域 DNS」黑名單
當 MAC 位址在 2 小時或以內與三個以上的不同 NetBIOS 主機名稱相關聯時	將 MAC 位址新增至資產核對網域 MAC 黑名單

您可以在**攻擊**標籤上檢視這些規則，方法爲按一下**規則**，然後在下拉清單中選取**資產核對排除**群組。

相關概念:

『範例：經調整將 IP 位址排除在黑名單外的資產排除規則』
透過調整資產排除規則，可以將 IP 位址排除列入黑名單。

範例：經調整將 IP 位址排除在黑名單外的資產排除規則

透過調整資產排除規則，可以將 IP 位址排除列入黑名單。

身爲網路安全管理者，您可以管理包含公用 wifi 網路區段（其中 IP 位址租賃通常既短又頻繁）的公司網路。 此網路區段上的資產傾向於暫時的，主要是經常登入及登出公用 wifi 的筆記型電腦和手持式裝置。 通常是不同裝置在短時間內使用單一 IP 位址多次。

在其餘的部署中，您擁有僅由庫存的、妥善命名的公司裝置組成的小心管理的網路。 在這個網路部分，IP 位址租賃的時間遠遠較久，且 IP 位址僅透過鑑別進行存取。 在此網路區段上，您想要立即得知何時有任何資產成長偏差，並想要保留資產核對排除規則的預設值。

將 IP 位址列入黑名單

在此環境中，預設資產核對排除規則會在短時間內無意間將整個網路列入黑名單。

您的安全團隊發現 wifi 區段所產生的資產相關通知是一件麻煩的事。 您想要防止 wifi 再觸發任何偏差的資產成長通知。

調整資產核對規則以忽略部分資產更新項目

您檢閱前次系統通知中的**依日誌來源的資產偏差**報告。 您判定被列入黑名單的資料是來自 wifi 上的 DHCP 伺服器。

對應於 **AssetExclusion：依 MAC 位址排除 IP**規則之列的**事件計數**直欄、**流程計數**直欄和**攻擊**直欄中的值指出，您的 wifi DHCP 伺服器正在觸發此規則。

您將測試新增至現有的資產核對排除規則，以停止規則將 wifi 資料新增至黑名單。

```
Apply AssetExclusion:Exclude IP by MAC address on events which are detected by
the Local system and NOT when the event(s) were detected by one or more of
MicrosoftDHCP @ microsoft.dhcp.test.com
and NOT when any of Domain is the key and any of Identity IP is the value in
any of Asset Reconciliation Domain IPv4 Whitelist
- IP Asset Reconciliation Domain IPv4 Blacklist - IP
and when at least 3 events are seen with the same Identity IP and
different Identity MAC in 2 hours.
```

更新的規則僅測試日誌來源中不是在您的 wifi DHCP 伺服器上的事件。 若要防止 wifi DHCP 事件接受更昂貴的參照集和行爲分析測試，您也將此測試移至測試堆疊的頂端

資產合併

資產合併 (Asset merging) 是指在它們實際上是相同的實體資產的前提下，一個資產的資訊與另一個資產的資訊結合的程序。

當資產更新項目包含符合兩個不同資產設定檔的身分資料時，就會發生資產合併。 例如，包含的 NetBIOS 主機名稱符合一個資產設定檔以及 MAC 位址符合不同資產設定檔的單一更新項目可能會觸發資產合併。

部分系統可能會導致大量的資產合併，因爲它們具有的資產資料來源不愼將來自兩個不同實體資產中的身分資訊結合成單一資產更新項目。 這些系統的部分範例包含下列環境：

- 作爲事件 Proxy 的中央 syslog 伺服器
- 虛擬機器
- 自動化安裝環境
- 非唯一的主機名稱，常見於 iPad 和 iPhone 之類的資產。
- 具有共用 MAC 位址的虛擬專用網路
- 其中身分欄位爲 `OverrideAndAlwaysSend=true` 的日誌來源延伸

具有許多 IP 位址、MAC 位址或主機名稱的資產顯示資產成長上的偏差，並可能觸發系統通知。

相關概念:

第 104 頁的『識別資產成長偏差』

有時候，資產資料來源會產生一些更新項目，在沒有人爲補救的情況下，IBM Security QRadar 無法正確處理這些更新項目。視異常資產成長原因而定，您可以修正導致問題的資產資料來源，也可以封鎖來自該資料來源的資產更新項目。

識別資產成長偏差

有時候，資產資料來源會產生一些更新項目，在沒有人爲補救的情況下，IBM Security QRadar 無法正確處理這些更新項目。視異常資產成長原因而定，您可以修正導致問題的資產資料來源，也可以封鎖來自該資料來源的資產更新項目。

當單一裝置的資產更新項目數超過特定類型識別資訊的保留臨界值時，會發生*資產成長偏差 (Asset growth deviations)*。適當地處理資產成長偏差對於維護精確的資產模型而言很重要。

實質上，每個資產成長偏差是在更新資產模型時其資料不受信任的資產資料來源。識別潛在的資產成長偏差時，您必須查看資訊來源，以判定是否有合理的解釋來說明資產爲何累積大量身分資料。資產成長偏差的原因特定於環境。

資產設定檔中非自然資產成長的 DHCP 伺服器範例

考量「動態主機配置通訊協定 (DHCP)」網路中的虛擬私密網路 (VPN) 伺服器。 VPN 伺服器被配置爲指派 IP 位址給送入的 VPN 用戶端，方法爲代表用戶端向網路的 DHCP 伺服器代理 DHCP 要求。

站在 DHCP 伺服器的角度看來，是相同的 MAC 位址反覆地要求許多 IP 位址指派。在網路作業的環境定義中，VPN 伺服器正在委派 IP 位址給用戶端，但是當一個資產代表另一個資產提出要求時，DHCP 伺服器無法區分。

被配置爲 QRadar 日誌來源的 DHCP 伺服器日誌會產生 DHCP 確認通知 (DHCP ACK) 事件，該事件將 VPN 伺服器的 MAC 位址與它指派給 VPN 用戶端的 IP 位址產生關聯。 當資產核對發生時，系統會依 MAC 位址核對此事件，這導致現有的單一資產隨著所剖析的每個 DHCP ACK 事件各成長一個 IP 位址。

最終，一個資產設定檔包含每個配置給 VPN 伺服器的 IP 位址。 此資產成長偏差是由於包含多個資產的相關資訊之資產更新項目所導致。

臨界值設定

當資料庫中的資產達到特定數目的內容時（如多個 IP 位址或 MAC 位址），QRadar 會封鎖該資產接收更多更新項目。

「資產側寫程式臨界值」設定指定資產在其下遭封鎖接收更新項目的條件。 資產通常最多更新到臨界值。 當系統收集的資料足以超出臨界值時，資產就會顯示資產成長偏差。對於資產的進一步更新會遭到封鎖，直到成長案偏差被更正爲止。

指出資產成長偏差的系統通知

IBM Security QRadar 會產生系統通知，以幫助您識別及管理您環境中的資產成長偏差。

下列系統訊息指出 QRadar 確認了潛在的資產成長偏差：

- 系統偵測到超出正常大小臨界值的資產設定檔
- 資產黑名單規則已將新的資產資料新增至資產黑名單

系統通知訊息包含報告的鏈結，以幫助您識別有成長偏差的資產。

頻繁變更的資產資料

合法變更的大量資產資料可導致資產成長，例如在下列情況下：

- 行動式裝置頻繁地在辦公室間移動，無論何時登入都獲指派新的 IP 位址。
- 連接至使用短 IP 位址租約之公用 Wifi（例如在大學校區）的裝置，可能會在一學期內收集大量的資產資料。

範例：日誌來源延伸的配置錯誤會如何導致資產成長偏差

配置不適當的自訂日誌來源延伸可能會導致資產成長偏差。

您可以從中央日誌伺服器上的事件有效負載剖析使用者名稱，配置自訂的日誌來源延伸以提供資產更新項目給 QRadar。 您可以配置日誌來源延伸來置換事件主機名稱內容，讓自訂日誌來源所產生的資產更新項目一律指定中央日誌伺服器的 DNS 主機名稱。

日誌來源會產生許多主機名稱全部都相同的資產更新項目，而不是 QRadar 接收具有使用者登入之資產主機名稱的更新項目。

在此狀況下，一個包含許多 IP 位址和使用者名稱的資產設定檔會導致資產成長偏差。

疑難排解超出正常大小臨界值的資產設定檔

當單一資產下的資料累計超出配置的身分資料臨界值限制時，IBM Security QRadar 會產生下列系統通知。

系統偵測到超出正常大小臨界值的資產設定檔

說明

通知的內容顯示前五名最常偏差的資產清單，以及系統爲何將各個資產標示爲成長偏差的原因。 如下例所示，該內容還顯示資產試圖成長超過資產大小臨界值的次數。

```
Feb 13 20:13:23 127.0.0.1 [AssetProfilerLogTimer]
com.q1labs.assetprofile.updateresolution.UpdateResolutionManager:
[INFO] [NOT:0010006101][9.21.118.83/- -] [-/- -]
The top five most frequently deviating asset profiles between
Feb 13, 2015 8:10:23 PM AST and Feb 13, 2015 8:13:23 PM AST:
[ASSET ID:1003, REASON:Too Many IPs, COUNT:508],
[ASSET ID:1002, REASON:Too many DNS Names, COUNT:93],
[ASSET ID:1001, REASON:Too many MAC Addresses, COUNT:62]
```

當資產資料超出配置的臨界值時，QRadar 會封鎖資產進行將來的更新。 此人爲介入可防止系統接收更多毀損資料，並減少系統試圖比對異常大的資產設定檔來核對送入的更新項目所可能發生的效能衝擊。

必要的使用者動作

使用通知有效負載中的資訊識別造成資產成長偏差的資產，並判定什麼原因導致異常成長。 通知提供在過去 24 小時內遇到偏差的資產成長的所有資產的報告鏈結。

在解決您環境中的資產成長偏差之後，您就可以再度執行報告。

1. 按一下**日誌活動**標籤，然後按一下**搜尋 > 新搜尋**。
2. 選取**偏差的資產成長：資產報告**已儲存的搜尋。
3. 使用報告識別及修復在偏差期間所建立的不正確資產資料。

如果資產資料有效，QRadar 管理者可以在QRadar **管理**標籤上的**資產側寫程式配置**中，增加 IP 位址、MAC 位址、NetBIOS 主機名稱和 DNS 主機名稱的臨界值限制。

新的資產資料已新增至資產黑名單

當一段資產資料顯出與偏差的資產成長一致的行爲時，IBM Security QRadar 會產生下列系統通知。

資產黑名單規則已將新的資產資料新增至資產黑名單

說明

資產排除規則會監視資產資料是否一致及完整。 該規則會在一段時間內追蹤一些特定的資產資料，以確保在合理的時間內以相同的資料子集一致地觀察它們。

例如，如果資產更新項目同時包含 MAC 位址和 DNS 主機名稱，則在持續的期間，該 MAC 位址會與該 DNS 主機名稱相關聯。 當資產更新項目中包含 DNS 主機名稱時，包含該 MAC 位址的後續資產更新項目也會包含相同的 DNS 主機名稱。 如果 MAC 位址突然與不同的 DNS 主機名稱相關聯達一段短期間，則會監視變更。如果 MAC 位址在短期間內再度變更，則系統會將該 MAC 位址標示爲造成偏差或異常資產成長的實例。

必要的使用者動作

使用通知有效負載中的資訊識別用於監視資產資料的規則。 按一下通知中的**依日誌來源的資產偏差**鏈結，以查看在最近 24 小時內發生的資產偏差。

如果資產資料有效，QRadar 管理者可以配置 QRadar 來解決問題。

- 如果您的黑名單過於積極移入，可以調整移入它們的資產核對排除規則。
- 如果您要將資料新增至資產資料庫，可以從黑名單移除資產資料，然後將它新增至對應的資產白名單。 將資產資料新增至白名單可防止它無意間重新出現在黑名單上。

資產黑名單和白名單

IBM Security QRadar 使用一組資產核對規則來判定資產資料是否可信任。當資產資料受到質疑時，QRadar 使用資產黑名單和白名單來判定是否使用資產資料來更新資產設定檔。

資產黑名單 (asset blacklist) 是IBM Security QRadar 視爲不可信任的資料集合。資產黑名單中的資料很可能造成資產成長偏差，因此 QRadar 會防止該資料新增至資產資料庫。

資產白名單 (asset whitelist) 是用來置換資產核對引擎邏輯（關於將哪些資料加入資產黑名單）的資產資料集合。如果系統識別黑名單相符項，它會檢查白名單以查看是否存在該值。如果資產更新符合白名單上的資料，則會核對變更並更新資產。白名單資產資料會全部套用於所有網域。

QRadar 管理者可以修改資產黑名單與白名單資料以防止將來出現資產成長偏差。

資產黑名單

資產黑名單 (asset blacklist) 是指 IBM Security QRadar 根據資產核對排除規則認爲無法信任的資料集合。 資產黑名單中的資料很可能造成資產成長偏差，因此 QRadar 會防止該資料新增至資產資料庫。

系統會將 QRadar 中的每個資產更新項目與資產黑名單比較。 系統會針對所有網域廣域套用列入黑名單的資產資料。 如果資產更新項目包含黑名單上出現的身分資訊（MAC 位址、NetBIOS 主機名稱、DNS 主機名稱或 IP 位址），則會捨棄送入的更新項目，且不會更新資產資料庫。

下表顯示每一種類型的身分資產資料的參照收集名稱和類型。

表 31. 資產黑名單資料的參照收集名稱

身分資料的類型	參照收集名稱	參照收集類型
IP 位址 (v4)	資產核對 IPv4 黑名單	參照集 [集類型：IP]
DNS 主機名稱	資產核對 DNS 黑名單	參照集 [集類型：ALNIC*]
NetBIOS 主機名稱	資產核對 NetBIOS 黑名單	參照集 [集類型：ALNIC*]
MAC 位址	資產核對 MAC 黑名單	參照集 [集類型：ALNIC*]
* ALNIC 是一種英數類型，可同時容納主機名稱和 MAC 位址值。		

您的 QRadar 管理者可以修改黑名單項目以確保正確地處理新資產資料。

資產白名單

您可以使用資產白名單以防止 IBM Security QRadar 資產資料不小心重新出現在資產黑名單中。

*資產白名單*是用來置換資產核對引擎邏輯（關於將哪些資料加入資產白名單）的資產資料集合。如果系統識別黑名單相符項，它會檢查白名單以查看存在哪個值。如果資產更新符合白名單上的資料，則會核對變更並更新資產。白名單資產資料會全部套用於所有網域。

您的 QRadar 管理者可以修改白名單項目以確保正確地處理新資產資料。

白名單使用案例範例

如果您的資產資料是有效的資產更新，當它持續顯示在黑名單中時，白名單會很有用。例如，您可能有一個循環式 NDS 負載平衡器，配置爲循環一組 IP 位址（5 個）。「資產核對排除」規則可確定與同一 DNS 主機名稱相關聯的多個 IP 位址可指示資產成長偏差，而系統可將 DNS 負載平衡器新增至黑名單。若要解決此問題，您可以將 DNS 主機名稱新增至「資產核對 DNS 白名單」。

資產白名單的大量項目

精確的資產資料庫可讓您更輕易將在您系統中所觸發的攻擊連接至您網路中的實體或虛擬資產。透過將大量項目新增至資產白名單來忽略資產偏差，並不能協助建置精確的資產資料庫。請檢閱資產黑名單以判定是什麼造成資產成長偏差，然後決定如何修正，而不是新增大量白名單項目。

資產白名單的類型

每種類型的身分資料都保留在個別白名單中。下表顯示每一種類型的身分資產資料的參照收集名稱和類型。

表 32. 資產白名單資料的參照集合名稱

資料類型	參照收集名稱	參照收集類型
IP 位址	資產核對 IPv4 白名單	參照集 [集類型：IP]
DNS 主機名稱	資產核對 DNS 白名單	參照集 [集類型：ALNIC*]
NetBIOS 主機名稱	資產核對 NetBIOS 白名單	參照集 [集類型：ALNIC*]
MAC 位址	資產核對 MAC 白名單	參照集 [集類型：ALNIC*]
* ALNIC 是一種英數類型，可同時容納主機名稱和 MAC 位址值。		

資產設定檔頁面參數

您可以尋找「資產摘要」窗格、「網路介面」窗格、「漏洞」窗格、「服務」窗格、「套件」窗格、「Windows 修補程式」窗格、「內容」窗格、「風險原則」窗格及「產品」窗格的「資產設定檔」頁面參數說明。

此參照包含的表格說明**資產設定檔**標籤的每個窗格中顯示的參數。

資產設定檔

資產設定檔提供您網路中每一個已知資產的相關資訊，包括哪些服務正在各個資產上執行中。

系統會使用資產設定檔資訊以便產生關聯，以幫助減少誤判。 例如，如果來源嘗試利用資產上執行的特定服務，則 QRadar 會透過將此攻擊與資產設定檔產生關聯，來判定資產是否容易遭到此攻擊。

如果您已配置流程資料或漏洞評量 (VA) 掃描，則會自動探索資產設定檔。爲使流程資料移入資產設定檔，需要雙向流程。 您也可以透過身分事件自動建立資產設定檔。 如需 VA 的相關資訊，請參閱 *IBM Security QRadar Vulnerability Assessment Guide*。

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

漏洞

您可以使用 QRadar Vulnerability Manager 及第三方掃描程式來識別漏洞。

第三方掃描程式使用外部參照（如「開放程式碼漏洞資料庫 (OSVDB)」、「國家漏洞資料庫 (NVDB)」及 Critical Watch）識別及報告探索到的漏洞。第三方掃描程式的範例包括 QualysGuard 及 nCircle ip360。 OSVDB 會將唯一的參照 ID (OSVDB ID) 指派給每個漏洞。 外部參照會將唯一的參照 ID 指派給每個漏洞。 外部資料參照 ID 的範例包括「通用漏洞及披露 (CVE)」ID 或 Bugtraq ID。 如需掃描程式及漏洞評量的相關資訊，請參閱 *IBM Security QRadar Vulnerability Manager User Guide*。

QRadar Vulnerability Manager 是您可以單獨購買及使用授權金鑰啓用的元件。 QRadar Vulnerability Manager 是網路掃描平台，可提供網路上應用程式、系統或裝置內存在的漏洞狀態提示。在掃描識別漏洞之後，您可以搜尋及檢閱漏洞資料，補救漏洞，及重新執行掃描來評估新的風險層次。

啓用 QRadar Vulnerability Manager 時，您可以在**漏洞**標籤上執行漏洞評量作業。透過**資產**標籤，您可以對選取的資產執行掃描。

如需相關資訊，請參閱 *IBM Security QRadar Vulnerability Manager User Guide*

資產標籤概觀

資產標籤爲您提供了工作區，您可以從中管理網路資產，及調查資產的漏洞、埠、應用程式、歷程及其他關聯。

使用**資產**標籤，您可以：

- 檢視所有探索到的資產。
- 手動新增資產設定檔。
- 搜尋特定的資產。
- 檢視探索到的資產的相關資訊。
- 編輯手動新增或探索到的資產的資產設定檔。
- 調整誤判漏洞。
- 匯入資產。
- 列印或匯出資產設定檔。
- 探索資產。
- 配置及管理第三方漏洞掃描。
- 啓動 QRadar Vulnerability Manager 掃描。

如需導覽窗格中「伺服器探索」選項的相關資訊，請參閱 *IBM Security QRadar SIEM Administration Guide*

如需導覽窗格中「VA 掃描」選項的相關資訊，請參閱 *IBM Security QRadar Risk Manager User Guide*。

資產標籤清單

「資產設定檔」頁面提供了 ID、「IP 位址」、「資產名稱」、「聚集 CVSS 評分」、「漏洞」及「服務」的相關資訊。

「資產設定檔」頁面提供每個資產的下列相關資訊：

表 33. 資產設定檔頁面參數

參數	說明
ID	顯示資產的「資產 ID」號碼。 在您手動新增資產設定檔時，或在透過事件、流程或漏洞掃描探索資產時，會自動產生「資產 ID」號碼。
IP 位址	顯示資產的最後一個已知的 IP 位址。
資產名稱	顯示資產的給定名稱、NetBios 名稱、DSN 名稱或 MAC 位址。 如果不明，此欄位會顯示最後一個已知的 IP 位址。 **註**：這些值會以優先順序顯示。 例如，如果資產沒有給定名稱，畫面上會顯示聚集 NetBios 名稱。 如果自動探索資產，會自動移入此欄位，但是，您可以在需要時編輯資產名稱。

表 33. 資產設定檔頁面參數 (繼續)

參數	說明
風險評分	顯示下列其中一個「共用漏洞評分系統 (CVSS)」評分： • 聯合的聚集環境 CVSS 評分 • 聚集時間 CVSS 評分 • 聚集 CVSS 基本評分 • 這些評分會以優先順序顯示。 例如，如果聯合的聚集環境 CVSS 評分無法使用，畫面上會顯示聚集時間 CVSS 評分。 CVSS 評分是漏洞嚴重性的評量度量值。 您可以使用 CVSS 評分，來測量某個漏洞與其他漏洞相比的關注度。 根據下列使用者定義的參數計算 CVSS 評分： • 可能的附屬資料損壞 • 機密性需求 • 可用性需求 • 完整性需求 如需如何配置這些參數的相關資訊，請參閱第 113 頁的『新增或編輯資產設定檔』。 如需 CVSS 的相關資訊，請參閱 http://www.first.org/cvss/。
漏洞	顯示在此資產上探索的唯一漏洞數目。 此值也包含主動及被動漏洞的數目。
服務	顯示此資產上執行的唯一第 7 層應用程式數目。
最後一個使用者	顯示與資產相關聯的最後一個使用者。
最後看到的使用者	顯示前次查看與資產相關聯的最後一個使用者的時間。

右鍵功能表選項

用滑鼠右鍵按一下「資產」標籤上的資產會顯示數個功能表，以取得更多事件過濾器資訊。

在**資產**標籤上，您可以用滑鼠右鍵按一下資產以存取更多事件過濾器資訊。

表 34. 右鍵功能表選項

選項	說明
導覽	**導覽**功能表提供下列選項： • **依網路檢視** - 顯示「網路清單」視窗，此視窗會顯示與所選取 IP 位址相關聯的所有網路。 • **檢視來源摘要** - 顯示「攻擊清單」視窗，此視窗會顯示與所選取來源 IP 位址相關聯的所有攻擊。 • **檢視目的地摘要** - 顯示「攻擊清單」視窗，此視窗會顯示與所選取目的地 IP 位址相關聯的所有攻擊。
資訊	**資訊**功能表提供下列選項： • **DNS 查閱** - 搜尋基於 IP 位址的 DNS 項目。 • **WHOIS 查閱** - 搜尋遠端 IP 位址的登錄擁有者。 預設 WHOIS 伺服器爲 whois.arin.net。 • **埠掃描** - 執行所選取 IP 位址的 Network Mapper (NMAP) 掃描。只有在系統上已安裝 NMAP 時，此選項才可用。如需安裝 NMAP 的相關資訊，請參閱供應商文件。 • **資產設定檔** - 顯示資產設定檔資訊。 只有在掃描主動獲得或流程來源被動獲得設定檔資料時，此功能表選項才可用。 • **搜尋事件** - 選取**搜尋事件**選項可搜尋與此 IP 位址相關聯的事件。 • **搜尋流程** - 選取「搜尋流程」選項可搜尋與此 IP 位址相關聯的流程。
執行漏洞掃描	選取此選項可對選取的資產執行 Vulnerability Manager 掃描。 只有在您安裝 QRadar Vulnerability Manager 之後，才會顯示此選項。

檢視資產設定檔

從**資產**標籤上的資產清單中，可以選取並檢視資產設定檔。 資產設定檔提供每一個設定檔的相關資訊。

關於這項作業

資產設定檔資訊是透過「伺服器探索」自動探索到的，或手動配置的。您可以編輯自動產生的資產設定檔資訊。

「資產設定檔」頁面提供資產的相關資訊，並將其組織到數個窗格內。 若要檢視窗格，您可以按一下窗格上的箭頭 **(>)**，以檢視更多詳細資料，或從工具列上的**顯示**清單框選取窗格。

「資產設定檔」頁面工具列提供下列功能：

表 35. 「資產設定檔」頁面工具列功能

選項	說明
回到資產清單	按一下此選項，以回到資產清單。
顯示	從這個清單框中，您可以選取要在「資產設定檔」窗格上檢視的窗格。 一律顯示「資產摘要」及「網路介面摘要」窗格。 如需每一個窗格中顯示之參數的相關資訊，請參閱資產設定檔頁面參數。
編輯資產	按一下此選項以編輯「資產設定檔」。 請參閱第 113 頁的『新增或編輯資產設定檔』。
依網路檢視	如果該資產與攻擊相關聯，則此選項將容許您檢視與該資產相關聯的網路清單。 當您按一下**依網路檢視**時，則顯示「網路清單」視窗。 請參閱第 32 頁的『監視依網路分組的攻擊』。
檢視來源摘要	如果該資產爲攻擊的來源，則此選項將容許您檢視來源摘要資訊。 當您按一下**檢視來源摘要**時，則顯示「攻擊清單」視窗。 請參閱第 31 頁的『監視依來源 IP 分組的攻擊』。
檢視目的地摘要	如果該資產爲攻擊的目的地，則此選項將容許您檢視目的地摘要資訊。 當您按一下**檢視目的地摘要**時，則顯示「目的地清單」視窗。請參閱第 32 頁的『監視依目的地 IP 分組的攻擊』。
歷程	按一下**歷程**，以檢視該資產的事件歷程資訊。 當您按一下**歷程**圖示時，會顯示「事件搜尋」視窗，並以事件搜尋準則預先移入： 若有需要，您可以自訂搜尋參數。 按一下**搜尋**，以檢視事件歷程資訊。
應用程式	按一下**應用程式**，以檢視該資產的應用程式資訊。 當您按一下**應用程式**圖示時，會顯示「流程搜尋」視窗，並以事件搜尋準則預先移入。 若有需要，您可以自訂搜尋參數。 按一下**搜尋**，以檢視應用程式資訊。
搜尋連線	按一下**搜尋連線**，以搜尋連線。 顯示「連線搜尋」視窗。 僅當已購買 IBM Security QRadar Risk Manager 並得到授權之後才會顯示此選項。 如需相關資訊，請參閱 *IBM Security QRadar Risk Manager User Guide*。

表 35. 「資產設定檔」頁面工具列功能 (繼續)

選項	說明
檢視拓蹼	按一下**檢視拓蹼**，以進一步調查資產。 顯示「現行拓蹼」視窗。 僅當已購買 IBM Security QRadar Risk Manager 並得到授權之後才會顯示此選項。 如需相關資訊，請參閱 *IBM Security QRadar Risk Manager User Guide*。
動作	從**動作**清單中，選取**漏洞歷程**。 僅當已購買 IBM Security QRadar Risk Manager 並得到授權之後才會顯示此選項。 如需相關資訊，請參閱 *IBM Security QRadar Risk Manager User Guide*。

程序

1. 按一下**資產**標籤。
2. 在導覽功能表上，按一下**資產設定檔**。
3. 按兩下您要檢視的資產。
4. 使用工具列上的選項來顯示資產設定檔資訊的各窗格。 請參閱編輯資產設定檔。
5. 若要研究關聯的漏洞，請按一下「漏洞」窗格中的每一個漏洞。 請參閱表 10-10。
6. 如有需要，可編輯資產設定檔。 請參閱編輯資產設定檔。
7. 如有需要，按一下**回到資產清單**，以選取並檢視其他資產。

新增或編輯資產設定檔

資產設定檔可自動探索及新增；但是，您可能需要手動新增設定檔

關於這項作業

當使用「伺服器探索」選項探索到資產時，會自動移入一些資產設定檔詳細資料。 您可以手動將資訊新增至資產設定檔，並且可以編輯某些參數。

您只能編輯手動輸入的參數。 系統產生的參數會以斜體顯示，不能編輯。 若有需要，您可以刪除系統產生的參數。

程序

1. 按一下**資產**標籤。
2. 在導覽功能表上，按一下**資產設定檔**。
3. 選擇下列其中一個選項：
   - 若要新增資產，按一下**新增資產**，然後在**新 IP 位址**欄位中鍵入資產的 IP 位址或 CIDR 範圍。
   - 若要編輯資產，按兩下要檢視的資產，然後按一下**編輯資產**。
4. 在「MAC 與 IP 位址」窗格中配置參數。配置下列一或多個選項：
   - 按一下**新 MAC 位址**圖示，並在對話框中的鍵入 MAC 位址。
   - 按一下**新 IP 位址**圖示，並在對話框中的鍵入 IP 位址。
   - 如果列出了**不明 NIC**，則可以選取此項，按一下**編輯**圖示，然後在對話框中鍵入新的 MAC 位址。

- 從清單選取 MAC 或 IP 位址，按一下**編輯**圖示，然後在對話框中鍵入新的 MAC 位址。
- 從清單選取 MAC 或 IP 位址，然後按一下**移除**圖示。

5. 在「名稱與說明」窗格中配置參數。 配置下列一或多個選項：

參數	說明
DNS	選擇下列其中一個選項： • 鍵入 DNS 名稱，然後按一下**新增**。 • 從清單選取 DNS 名稱，然後按一下**編輯**。 • 從清單選取 DNS 名稱，然後按一下**移除**。
NetBIOS	選擇下列其中一個選項： • 鍵入 NetBIOS 名稱，然後按一下**新增**。 • 從清單選取 NetBIOS 名稱，然後按一下**編輯**。 • 從清單選取 NetBIOS 名稱，然後按一下**移除**。
給定名稱	鍵入此資產設定檔的名稱。
位置	鍵入此資產設定檔的位置。
說明	鍵入資產設定檔的說明。
無線 AP	鍵入此資產設定檔的無線「存取點 (AP)」。
無線 SSID	鍵入此資產設定檔的無線「服務集 ID (SSID)」。
交換器 ID	鍵入此資產設定檔的交換器 ID。
交換器埠 ID	鍵入此資產設定檔的交換器埠 ID。

6. 在「作業系統」窗格中配置參數：
   a. 從**供應商**清單框中，選取作業系統供應商。
   b. 從**產品**清單框中，選取資產設定檔的作業系統。
   c. 從**版本**清單框中，選取所選作業系統的版本。
   d. 按一下**新增**圖示。
   e. 從**置換**清單框中，選取下列其中一項：
      - **截止下一次掃描** - 選取此選項以指定掃描器提供作業系統資訊，且可以臨時編輯該資訊。 如果您編輯了作業系統參數，則掃描器會在其下一次掃描時還原資訊。
      - **永久** - 選取此選項以指定您要手動輸入作業系統資訊，並停用掃描器更新資訊。
   f. 從清單選取作業系統。
   g. 選取作業系統，然後按一下**切換置換**圖示。
7. 在「CVSS 與加權」窗格中配置參數。配置下列一或多個選項：

參數	說明
可能的附屬資料損壞	配置此參數來指示因損壞或竊取此資產可能導致生命或實體資產流失。 您還可以使用此參數來指示可能導致生產力或收益的經濟流失。 增加對關聯損壞的可能性會增加「CVSS 評分」參數中的計算值。 從**關聯損壞可能**清單框中，選取下列其中一項： • 無 • 低 • 低中 • 中高 • 高 • 未定義 當您配置**關聯損壞可能**參數時，會自動更新**加權**參數。
機密性需求	配置此參數來指示成功利用這個資產漏洞的機密性的影響。 增加對機密性的影響會增加「CVSS 評分」參數中的計算值。 從**機密性需求**清單框中，選取下列其中一項： • 低 • 中 • 高 • 未定義
可用性需求	配置此參數來指示成功利用這個漏洞時對資產可用性的影響。 耗用網路頻寬、處理器週期或磁碟空間的攻擊會影響資產的可用性。 增加對可用性的影響會增加「CVSS 評分」參數中的計算值。 從**可用性需求**清單框中，選取下列其中一項： • 低 • 中 • 高 • 未定義

參數	說明
完整性需求	配置此參數來指示成功利用這個漏洞時對資產完整性的影響。 完整性是指資訊的可信度和保證的眞實性。 增加對完整性的影響會增加「CVSS 評分」參數中的計算值。 從**完整性需求**清單框中，選取下列其中一項： • 低 • 中 • 高 • 未定義
加權	從**加權**清單框中，選取該資產設定檔的加權。範圍爲 0 - 10。 當您配置**加權**參數時，會自動更新**關聯損壞可能**參數。

8. 在「擁有者」窗格中配置參數。 選擇下列一或多個選項：

參數	說明
事業擁有者	鍵入資產的業務擁有者名稱。 例如，業務擁有者爲部門經理。 最大長度爲 255 個字元。
業務擁有者聯絡人	鍵入業務擁有者的聯絡資訊。 最大長度爲 255 個字元。
技術擁有者	鍵入資產的技術擁有者。 例如，業務擁有者爲 IT 經理或主管。 最大長度爲 255 個字元。
技術擁有者聯絡人	鍵入技術擁有者的聯絡資訊。 最大長度爲 255 個字元。
技術使用者	從清單框中，選取您要與此資產設定檔相關聯的使用者名稱。 您還可以使用此參數來啓用 IBM Security QRadar Vulnerability Manager 的自動漏洞補救。如需自動補救的相關資訊，請參閱 *IBM Security QRadar Vulnerability Manager User Guide*。

9. 按一下**儲存**。

搜尋資產設定檔

您可以配置搜尋參數，以僅顯示要從**資產**標籤上的「資產」頁面調查的資產設定檔。

關於這項作業

當您存取**資產**標籤時，會顯示「資產」頁面，並移入在您網路中探索到的所有資產。 若要細化這個清單，您可以配置搜尋參數，以僅顯示您要調查的資產設定檔。

您可以從「資產搜尋」頁面管理「資產搜尋群組」。 如需「資產搜尋群組」的相關資訊，請參閱資產搜尋群組。

搜尋功能將容許您搜尋主機設定檔、資產及識別資訊。 識別資訊會提供您網路上日誌來源的更多明細，包括 DNS 資訊、使用者登入及 MAC 位址。

您可以使用資產搜尋功能來依外部資料參照搜尋資產，以判定您的部署中是否存在已知的漏洞。

例如：

您接收到通知，指示欄位中正在使用 CVE ID: CVE-2010-000。 若要驗證您的部署中是否有任何主機容易遭到此用法的攻擊，則可以從搜尋參數清單選取**漏洞外部參照**，選取 **CVE**，然後鍵入

```
2010-000
```

。

檢視容易遭到特定 CVE ID 攻擊的所有主機清單。

註：如需 OSVDB 的相關資訊，請參閱 *http://osvdb.org/*。如需 NVDB 的相關資訊，請參閱 *http://nvd.nist.gov/*。

程序

1. 按一下**資產**標籤。
2. 在導覽功能表上，按一下**資產設定檔**。
3. 在工具列上，按一下**搜尋 > 新搜尋**。
4. 選擇下列其中一個選項：
   - 若要載入之前儲存的搜尋，請跳至第 5 步。
   - 若要建立新搜尋，請跳至第 6 步。
5. 選取之前已儲存的搜尋：
   a. 選擇下列其中一個選項：
      - 選用項目。 從**群組**清單框中，選取要在**可用的已儲存搜尋**清單中顯示的資產搜尋群組。
      - 從**可用的已儲存搜尋**清單，選取要載入的已儲存搜尋。
      - 在**鍵入已儲存的搜尋或從清單選取**欄位中，鍵入要載入的搜尋名稱。
   b. 按一下**載入**。
6. 在「搜尋參數」窗格中，定義您的搜尋準則：
   a. 從第一個清單框中，選取要搜尋的資產參數。 例如，**主機名稱**、**漏洞風險分類**，或**技術擁有者**。
   b. 從第二個清單框中，選取您要用於搜尋的修飾元。
   c. 在輸入欄位中，鍵入與您的搜尋參數相關的特定資訊。
   d. 按一下**新增過濾器**。
   e. 對於要新增至搜尋準則的每一個過濾器，重複這些步驟。
7. 按一下**搜尋**。

結果

您可以儲存您的資產搜尋準則。 請參閱儲存資產搜尋準則。

儲存資產搜尋準則

在**資產**標籤上，您可以儲存配置的搜尋準則，以便可以重複使用該準則。 已儲存的搜尋準則不會到期。

程序

1. 按一下**資產**標籤。
2. 在導覽功能表上，按一下**資產設定檔**。
3. 執行搜尋。
4. 按一下**儲存準則**。
5. 輸入參數的值：

參數	說明
輸入該搜尋的名稱	鍵入要指派給這個搜尋準則的唯一名稱。
管理群組	按一下**管理群組**來管理搜尋群組。 僅當您具有管理許可權時，才會顯示這個選項。
將搜尋指派給群組	請選取要指派這個已儲存的搜尋的群組的勾選框。 如果不選取群組，則會依預設將這個已儲存的搜尋指派給**其他**群組。
包含在我的快速搜尋中	選取此勾選框以在**資產**標籤工具列上的**快速搜尋**清單框中包含此搜尋。
設為預設值	選取此勾選框來將此搜尋設定爲存取**資產**標籤時的預設搜尋。
與每個人共用	選取此勾選框來與所有使用者共用這些搜尋需求。

資產搜尋群組

使用「資產搜尋群組」視窗，您可以建立及管理資產搜尋群組。

這些群組可讓您輕鬆地在**資產**標籤上尋找已儲存的搜尋準則。

檢視搜尋群組

使用「資產搜尋群組」視窗檢視列出的群組和子群組。

關於這項作業

您可以從「資產搜尋群組」視窗，檢視每一個群組的詳細資料，包括說明和群組的前次修改日期。

所有未指派給群組的已儲存搜尋位於**其他**群組內。

「資產搜尋群組」視窗顯示每一個群組的下列參數：

表 36. 「資產搜尋群組」視窗工具列功能

功能	說明
新群組	若要建立新搜尋群組，可以按一下**新群組**。 請參閱建立新搜尋群組。

表 36. 「資產搜尋群組」視窗工具列功能 (繼續)

功能	說明
編輯	若要編輯現有搜尋群組，可以按一下**編輯**。 請參閱編輯搜尋群組。
複製	若要將已儲存的搜尋複製到其他搜尋群組，可以按一下**複製**。 請參閱將已儲存的搜尋複製到其他群組。
移除	若要移除搜尋群組，或從搜尋群組移除已儲存的搜尋，請選取要移除的項目，然後按一下**移除**。 請參閱移除群組，或從群組移除已儲存的搜尋。

程序

1. 按一下**資產**標籤。
2. 在導覽功能表上，按一下**資產設定檔**。
3. 選取**搜尋 > 新搜尋**。
4. 按一下**管理群組**。
5. 檢視搜尋群組。

建立新搜尋群組

在「資產搜尋群組」視窗上，可以建立新搜尋群組。

程序

1. 按一下**資產**標籤。
2. 在導覽功能表上，按一下**資產設定檔**。
3. 選取**搜尋 > 新搜尋**。
4. 按一下**管理群組**。
5. 選取要在其下建立新群組的群組資料夾。
6. 按一下**新群組**。
7. 在**名稱**欄位中，鍵入新群組的唯一名稱。
8. 選用項目。 在**說明**欄位中，鍵入說明。
9. 按一下**確定**。

編輯搜尋群組

您可以編輯搜尋群組的**名稱**與**說明**欄位。

程序

1. 按一下**資產**標籤。
2. 在導覽功能表上，按一下**資產設定檔**。
3. 選取**搜尋 > 新搜尋**。
4. 按一下**管理群組**。
5. 選取您要編輯的群組。
6. 按一下**編輯**。

7. 在**名稱**欄位中鍵入新名稱。
8. 在**說明**欄位中鍵入新說明。
9. 按一下**確定**。

將已儲存的搜尋複製到另一個群組

您可以將已儲存的搜尋複製到另一個群組。 還可以將已儲存的搜尋複製到多個群組。

程序

1. 按一下**資產**標籤。
2. 在導覽功能表上，按一下**資產設定檔**。
3. 選取**搜尋 > 新搜尋**。
4. 按一下**管理群組**。
5. 選取要複製的已儲存搜尋。
6. 按一下**複製**。
7. 在「項目群組」視窗中，選取要作爲已儲存的搜尋複製目的地之群組的勾選框。
8. 按一下**指派群組**。

移除群組或從群組移除已儲存的搜尋

您可以使用**移除**圖示從群組移除搜尋或移除搜尋群組。

關於這項作業

當您從群組移除已儲存的搜尋時，不會從系統刪除已儲存的搜尋。已儲存的搜尋將從群組移除，並自動移至**其他**群組。

您無法從系統移除下列群組：

- 資產搜尋群組
- 其他

程序

1. 按一下**資產**標籤。
2. 在導覽功能表上，按一下**資產設定檔**。
3. 選取**搜尋 > 新搜尋**。
4. 按一下**管理群組**。
5. 選取要從群組移除的已儲存的搜尋：
   - 選取要從群組移除的已儲存的搜尋。
   - 選取您要移除的群組。

資產設定檔管理作業

您可以使用「資產」標籤刪除、匯入及匯出資產設定檔。

關於這項作業

使用**資產**標籤，您可以刪除、匯入及匯出資產設定檔。

刪除資產

您可以刪除特定資產或所有列出的資產設定檔。

程序

1. 按一下**資產**標籤。
2. 在導覽功能表上，按一下**資產設定檔**。
3. 選取要刪除的資產，然後從**動作**清單框選取**刪除資產**。
4. 按一下**確定**。

匯入資產設定檔

您可以匯入資產設定檔資訊。

開始之前

匯入的檔案必須是採用下列格式的 CSV 檔案：

```
ip,name,weight,description
```

其中：

- **IP** - 指定任何帶點十進位格式的有效 IP 位址。 例如：192.168.5.34。
- **名稱** - 指定此資產的名稱，長度最多爲 255 個字元。 逗點在此欄位中無效，會使匯入處理程序失效。 例如：WebServer01 是不正確的。
- **加權** - 指定 0 到 10 的數字，指出此資產在您網路上的重要性。值 0 表示低重要性，值 10 表示高重要性。
- **說明** - 指定此資產的文字說明，長度最多爲 255 個字元。 此值是選用項目。

例如，CSV 檔案中可能包含下列項目：

-
  ```
  192.168.5.34,WebServer01,5,Main Production Web Server
  ```
-
  ```
  192.168.5.35,MailServ01,0,
  ```

匯入處理程序會將匯入的資產設定檔與目前儲存在系統中的資產設定檔資訊合併。

程序

1. 按一下**資產**標籤。
2. 在導覽功能表上，按一下**資產設定檔**。
3. 從**動作**清單框中，選取**匯入資產**。
4. 按一下**瀏覽**以尋找並選取要匯入的 CSV 檔。
5. 按一下**匯入資產**，以開始匯入處理程序。

匯出資產

您可以將所列的資產設定檔匯出爲「延伸標記語言 (XML)」或「以逗點區隔值 (CSV)」檔案。

程序

1. 按一下**資產**標籤。
2. 在導覽功能表上，按一下**資產設定檔**。
3. 從**動作**清單框中，選取下列其中一項：
   - 匯出至 XML
   - 匯出至 CSV
4. 檢視狀態視窗，以瞭解匯出處理程序的狀態。
5. 選擇性的： 若要在匯出進行時使用其他標籤及頁面，請按一下**完成時通知**鏈結。

   匯出完成時，會顯示「檔案下載」視窗。
6. 在「檔案下載」視窗上，選擇下列其中一個選項：
   - **開啓** - 選取此選項在您選擇的瀏覽器中開啓匯出結果。
   - **儲存** - 選取此選項將結果儲存到桌面上。
7. 按一下**確定**。

研究資產漏洞

「資產設定檔」頁面上的「漏洞」窗格可顯示探索到的資產漏洞清單。

關於這項作業

您可以按兩下漏洞，來顯示漏洞的更多詳細資料。

「研究漏洞詳細資料」視窗提供下列詳細資料：

參數	說明
漏洞 ID	指定漏洞的 ID。 「漏洞 ID」是「漏洞資訊系統 (VIS)」產生的唯一 ID。
已發佈日期	指定在 OSVDB 上發佈漏洞詳細資料的日期。
名稱	指定漏洞的名稱。
資產	指定您網路中有此漏洞的資產數。 按一下鏈結可檢視資產清單。
資產，包括異常狀況	指定您網路中有漏洞異常狀況的資產數。 按一下鏈結可檢視資產清單。
CVE	指定漏洞的 CVE ID。 CVE ID 由 NVDB 提供。 按一下鏈結以取得更多資訊。 當您按一下此鏈結時，會在新的瀏覽器視窗中顯示 NVDB 網站。
xforce	指定漏洞的 X-Force ID。 按一下鏈結以取得更多資訊。 當您按一下此鏈結時，會在新的瀏覽器視窗中顯示 IBM Internet Security Systems 網站。

參數	說明
OSVDB	指定漏洞的 OSVDB ID。 按一下鏈結以取得更多資訊。 當您按一下此鏈結時，會在新的瀏覽器視窗中顯示 OSVDB 網站。
外掛程式詳細資料	指定 QRadar Vulnerability Manager ID。 按一下鏈結以檢視漏洞的 Oval 定義、Windows 知識庫項目或 UNIX 建議。 此功能提供在修補程式掃描期間，QRadar Vulnerability Manager 如何檢查以取得漏洞詳細資料的相關資訊。 您可以使用它來識別資產上爲何出現或不出現漏洞的原因。
CVSS 評分基礎	顯示該資產上漏洞的聚集「共用漏洞評分系統 (CVSS)」評分。 CVSS 評分是漏洞嚴重性的評量度量值。您可以使用 CVSS 評分來測量某個漏洞較之其他漏洞的嚴重性如何。 利用下列使用者定義的參數來計算 CVSS 評分： • 可能的附屬資料損壞 • 機密性需求 • 可用性需求 • 完整性需求 如需如何配置這些參數的相關資訊，請參閱第 113 頁的『新增或編輯資產設定檔』。 如需 CVSS 的相關資訊，請參閱 *http://www.first.org/cvss/*。
影響	顯示若利用此漏洞，可以預期的損害或損壞類型。
CVSS 基本度量	顯示用於計算 CVSS 基本評分的度量值，包括： • 存取向量 • 存取複雜性 • 鑑別 • 機密性影響 • 完整性影響 • 可用性影響
說明	指定偵測到的漏洞的說明。 僅當您的系統整合 VA 工具時，此值才可用。
顧慮	指定漏洞可能對您的網路造成的影響。
解決方案	請遵循提供的指示來解決漏洞。

參數	說明
虛擬修補	顯示與此漏洞相關聯的虛擬修補程式資訊（若有）。虛擬修補程式是最近探索的漏洞的短期緩解解決方案。 本資訊衍生自「入侵保護系統 (IPS)」事件。 如果要安裝虛擬修補程式，請參閱您的 IPS 供應商資訊。
參照	顯示外部參照清單，包括： • **參照類型** - 指定所列的參照類型，例如：諮詢 URL 或郵件貼文清單。 • **URL** - 指定可以按一下以檢視參照的 URL。 按一下鏈結以取得更多資訊。當您按一下此鏈結時，會在新的瀏覽器視窗中顯示外部資源。
產品	顯示與此漏洞相關聯的產品清單。 • **供應商** - 指定產品的供應商。 • **產品** - 指定產品名稱。 • **版本** - 指定產品的版本號碼。

程序

1. 按一下**資產**標籤。
2. 在導覽功能表上，按一下**資產設定檔**。
3. 選取資產設定檔。
4. 在「漏洞」窗格中，對於您要調查的漏洞，按一下 **ID** 或**漏洞**參數值。

第 8 章 圖表管理

您可以使用各種圖表配置選項檢視資料。

您可以使用**日誌活動**及**網路活動**標籤上的圖表，利用各種圖表配置選項來檢視資料。

圖表管理

您可以使用各種圖表配置選項來檢視資料。

如果您選取時間範圍或分組選項來檢視資料，則圖表會顯示在事件或流程清單上方。

在串流模式下，圖表不會顯示。

您可以配置圖表以選取要繪製的資料。 您可以配置各自獨立的圖表，以從不同角度顯示您的搜尋結果。

圖表類型包括：

- 長條圖 - 以長條圖顯示資料。 此選項僅適用於分組事件。
- 圓餅圖 - 以圓餅圖顯示資料。 此選項僅適用於分組事件。
- 表格 - 以表格顯示資料。 此選項僅適用於分組事件。
- 時間序列 - 顯示互動式折線圖，來代表符合指定時間間隔的記錄。如需配置時間序列搜尋準則的相關資訊，請參閱時間序列圖表概觀。

配置圖表之後，在下列情況下會保留您的圖表配置：

- 使用**顯示**清單框來變更視圖。
- 套用過濾器。
- 儲存搜尋準則。

在下列情況下不會保留您的圖表配置：

- 啓動新搜尋。
- 存取快速搜尋。
- 在分支視窗中檢視分組結果。
- 儲存搜尋結果。

註：如果您使用 Mozilla Firefox Web 瀏覽器，且已安裝廣告封鎖程式瀏覽器延伸，則圖表不會顯示。 若要顯示圖表，您必須移除廣告封鎖程式瀏覽器延伸。 如需相關資訊，請參閱瀏覽器文件。

時間序列圖表概觀

時間序列圖表是一段時間內的活動的圖形表示法。

圖表中顯示的尖峰及谷值描述大量及少量活動。 時間序列圖表對於短期及長期資料趨勢很有用。

使用時間序列圖表，您可以存取、導覽及調查各種視圖及視景中的日誌或網路活動。

註：您必須具有適當的角色許可權，才能管理及檢視時間序列圖表。

若要顯示時間序列圖表，您必須建立及儲存包含時間序列和分組選項的搜尋。 您可以儲存多達 10 個時間序列搜尋。

您可以從事件或流程搜尋頁面上的可用搜尋清單存取預設時間序列儲存的搜尋。

您可以輕鬆地識別**快速搜尋**功能表上的已儲存時間序列搜尋，因爲搜尋名稱會附加在搜尋準則中指定的時間範圍內。

如果您的搜尋參數與直欄定義及分組選項的之前儲存的搜尋相符，搜尋結果的時間序列圖表可能會自動顯示。 如果未儲存的搜尋準則的時間序列圖表沒有自動顯示，則不存在與您的搜尋參數相符的之前儲存的搜尋準則。 如果發生此情況，您必須啓用時間序列資料擷取，並儲存您的搜尋準則。

您可以放大及掃描時間序列上的時間表來調查活動。 下表提供了您可以用於檢視時間序列圖表的功能。

表 37. 時間序列圖表功能

功能	說明
更詳細檢視資料	使用縮放功能，您可以調查事件資料流量的更小時段。 • 將滑鼠指標移在圖表上，然後使用滑鼠滾輪放大圖表（向上滾動滑鼠滾輪）。 • 強調顯示您要放大的圖表區域。 在您釋放滑鼠按鈕時，圖表會顯示更小的時段。現在，您可以按一下並拖曳圖表以掃描圖表。 在您放大時間序列圖表時，圖表會重新整理以顯示更小的時段。
檢視資料的更大時間跨距	使用縮放功能，您可以調查更大時段或回到最大時間範圍。 您可以使用下列其中一個選項來展開時間範圍： • 按一下圖表左上角的「重設縮放」。 • 將滑鼠指標移在圖表上，然後使用滑鼠滾輪展開視圖（向下滾動滑鼠滾輪）。
掃描圖表	已放大時間序列圖表時，您可以按一下並拖曳圖表至左側或右側來掃描時間表。

圖表圖註

每個圖表都提供圖註，圖註是視覺化參照，可協助您將圖表物件與其代表的參數相關聯。

使用圖註功能，您可以執行下列動作：

- 將滑鼠指標移在圖註項目或圖註顏色區塊上方，以檢視其代表的參數的相關資訊。
- 用滑鼠右鍵按一下圖註項目，以進一步調查此項目。
- 按一下圓餅圖或長條圖圖註項目，以隱藏圖表中的項目。再次按一下圖註項目，以顯示隱藏的項目。 您也可以按一下對應圖形項目，來隱藏及顯示此項目。

- 按一下**圖註**或其旁邊的箭頭（如果您要從圖表顯示中移除圖註）。

配置圖表

您可以使用配置選項來變更圖表類型、您要圖表化的物件，以及圖表上代表的物件數目。 對於時間序列圖表，您也可以選取時間範圍及啓用時間序列資料擷取。

開始之前

您在即時（串流）模式下檢視事件或流程時，不會顯示圖表。若要顯示圖表，您必須存取**日誌活動** 或 **網路活動**標籤，然後選擇下列其中一個選項：

- 從**檢視**及**顯示**清單框中選取選項，然後按一下工具列上的**儲存準則**。 請參閱儲存搜尋準則。
- 在工具列上，從**快速搜尋**清單中選取已儲存的搜尋。
- 執行分組搜尋，然後按一下工具列上的**儲存準則**。

如果您計劃配置時間序列圖表，請確保已儲存的搜尋準則已分組，並指定時間範圍。

關於這項作業

您可以累計資料，從而在執行時間序列搜尋時，可使用資料快取來顯示先前時段的資料。 對選取的參數啓用時間序列資料擷取之後，「要圖形化的值」清單框中的參數旁邊會顯示星號 (*)。

程序

1. 按一下**日誌活動** 或**網路活動**標籤。
2. 在「圖表」窗格中，按一下**配置**圖示。
3. 配置下列參數的值：

選項	敘述
參數	說明
要圖形化的值	從清單框中，選取您要在圖表的 Y 軸上圖形化的物件類型。 選項包括搜尋參數中包含的所有正規化及自訂事件或流程參數。
顯示前幾個	從清單框中，選取您要在圖表中檢視的物件數目。 預設值爲 10。 圖表化任何 10 個以上項目可能會導致圖表資料無法讀取。
圖表類型	從清單框中，選取您要檢視的圖表類型。 如果您的長條圖、圓餅圖或表格圖表基於已儲存的搜尋準則，且時間範圍超過 1 小時，您必須按一下**更新詳細資料**來更新圖表及移入事件詳細資料

選項	敘述
擷取時間序列資料	如果您要啓用時間序列資料擷取，請選取此勾選框。 在您選取此勾選框時，圖表功能會開始累計時間序列圖表的資料。 依預設，此選項已停用。 只有「時間序列」圖表才提供此選項。
時間範圍	從清單框中，選取您要檢視的時間範圍。 只有「時間序列」圖表才提供此選項。

4. 如果您已選取**時間序列**圖表選項及啓用**擷取時間序列資料**選項，請按一下工具列上的**儲存準則**。
5. 若要在時間範圍大於 1 小時的情況下檢視事件或流程清單，請按一下**更新詳細資料**。

第 9 章 資料搜尋

在**日誌活動**、**網路活動**及**攻擊**標籤上，您可以使用特定的準則搜尋事件、流程及攻擊。

您可以建立新搜尋或載入先前儲存的一組搜尋準則。 您可以選取、組織及分組要顯示在搜尋結果中的資料直欄。

事件和流程搜尋

您可以在**日誌活動** 及**網路活動**標籤上執行搜尋。

在執行搜尋之後，您可以儲存搜尋準則及搜尋結果。

搜尋符合準則的項目

您可以搜尋符合搜尋準則的資料。

關於這項作業

由於要搜尋整個資料庫，所以視您的資料庫大小而定，搜尋可能需要較長時間。

您可以使用**快速過濾器**搜尋參數來搜尋符合事件有效負載中的字串的項目。

下表說明了可以用來搜尋事件與流程資料的搜尋選項：

表 38. 搜尋選項

選項	說明
分組	選取事件搜尋群組或流程搜尋群組，以在**可用的已儲存搜尋**清單中檢視。
鍵入已儲存的搜尋或從清單選取	鍵入已儲存的搜尋名稱或關鍵字，以過濾**可用的已儲存搜尋**清單。
可用的已儲存的搜尋	此清單會顯示所有可用的搜尋，除非您使用**分組或鍵入已儲存的搜尋**或**從清單選取**選項來過濾清單。 您可以選取這個清單上某個已儲存的搜尋來顯示或編輯。
搜尋	**搜尋**圖示在搜尋頁面上的多個窗格內提供。 您可以在完成配置搜尋並希望檢視結果時按一下「搜尋」。
包含在我的快速搜尋中	選取此勾選框以在**快速搜尋**功能表中包含此搜尋。
包含在我的儀表板中	選取此勾選框以在**儀表板**標籤上包含已儲存的搜尋資料。 如需**儀表板**標籤的相關資訊，請參閱儀表板管理。 **註**：僅當對搜尋進行分組時才會顯示這個參數。
設爲預設值	選取此勾選框來將此搜尋設定爲預設的搜尋。

表 38. 搜尋選項 (繼續)

選項	說明
與每個人共用	選取此勾選框來與所有其他使用者共用此搜尋。
即時（串流）	顯示串流模式的結果。 如需串流模式的相關資訊，請參閱檢視串流事件。 **註**：當啓用「即時」（串流）時，無法分組搜尋結果。 如果在「直欄定義」窗格中選取任何分組選項，則會開啓錯誤訊息。
前次間隔（自動重新整理）	顯示自動重新整理模式的搜尋結果。 在自動重新整理模式中，**日誌活動** 及**網路活動**標籤會以一分鐘間隔重新整理以顯示最近資訊。
最近	選取您要搜尋的預先定義時間範圍。選取此選項之後，必須從清單框選取一個時間範圍選項。
特定的間隔	選取您要搜尋的自訂時間範圍。選取此選項之後，必須從**開始時間**和**結束時間**行事曆選取日期和時間範圍。
資料累積	僅當您載入已儲存的搜尋時才會顯示這個窗格。 在與許多其他已儲存搜尋及報告共用的累計資料上啓用唯一計數，可能會降低系統效能。 當您載入已儲存的搜尋時，此窗格會顯示下列選項： • 如果對此已儲存的搜尋沒有累計資料，則會顯示下列參考訊息：**對此搜尋沒有累計資料**。 • 如果對此已儲存的搜尋有累計資料，則會顯示下列選項： – **直欄** - 當您按一下此鏈結或將滑鼠移至此鏈結時，會開啓累計資料的直欄清單。 – **啓用唯一計數/停用唯一計數** - 此鏈結容許您啓用或停用搜尋結果，以顯示唯一事件與流程計數，而不是一段時間的平均計數。 按一下**啓用唯一計數**鏈結之後，會開啓一個對話框，並指示哪些已儲存的搜尋與報告共用累計資料。
現行過濾器	這個清單顯示套用至此搜尋的過濾器。 新增過濾器的選項位於**現行過濾器**清單上方。
搜尋完成時儲存結果。	選取此勾選框來儲存和命名搜尋結果。
顯示	選取此清單以指定設定爲在搜尋結果內顯示的預先定義的直欄。

表 38. 搜尋選項 (繼續)

選項	說明
鍵入直欄或從清單選取	您可以使用欄位來過濾「可用的直欄」清單中所列的直欄。 鍵入要尋找的直欄名稱，或鍵入關鍵字，以顯示直欄名稱的清單。 例如，鍵入 Device，以顯示直欄名稱中包含 Device 的直欄清單。
可用的直欄	此清單顯示可用的直欄。 這個已儲存的搜尋目前使用中的直欄會在**直欄**清單中強調顯示。
新增和移除直欄圖示（頂端集合）	使用頂端的一組圖示來自訂**分組依據**清單。 • **新增直欄** - 從**可用的直欄**清單中選取一或多個直欄，然後按一下**新增直欄**圖示。 • **移除直欄** - 從**分組依據**清單中選取一或多個直欄，然後按一下**移除直欄**圖示。
新增和移除直欄圖示（底端集合）	使用底端的一組圖示來自訂**直欄**清單。 • **新增直欄** - 從「可用的直欄」清單中選取一或多個直欄，然後按一下**新增直欄**圖示。 • **移除直欄** - 從「直欄」清單中選取一或多個直欄，然後按一下**移除直欄**圖示。
分組依據	此清單指定已儲存的搜尋要對其結果分組的直欄。 使用下列選項來進一步自訂「分組依據」清單： • 上移 - 選取一個直欄，並使用**上移**圖示在優先順序清單中將其向上移動。 • 下移 - 選取一個直欄，並使用**下移**圖示在優先順序清單中將其向下移動。 優先順序清單指定結果的分組順序。 搜尋結果將依**分組依據**清單中的第一個直欄分組，然後依清單中的下一個直欄分組。
直欄	指定選擇搜尋的直欄。您可以從**可用的直欄**清單中選取多個直欄。可以使用下列選項來進一步自訂**直欄**清單： • **上移** - 將所選的直欄在優先順序清單中向上移動。 • **下移** - 將所選的直欄在優先順序清單中向下移動。 如果直欄類型爲數字或基於時間，且**分組依據**清單中有項目，則該直欄包含清單框。 使用清單框來選擇如何分組直欄。 如果直欄如果直欄類型爲群組，則該直欄包含清單框，以便選擇針對群組要包含的層次數目。
排序方式	從第一個清單框中，選取要作爲搜尋結果排序依據的直欄。 然後，從第二個清單框中，選取搜尋結果的顯示順序。選項包括**降冪**和**升冪**。

表 38. 搜尋選項 (繼續)

選項	說明
結果限制	您可以在「編輯搜尋」視窗上指定搜尋返回的列數。 **結果限制**欄位還會出現在「結果」視窗上。 • 對於已儲存的搜尋，限制儲存在已儲存的搜尋內，並將在載入搜尋時重新套用。 • 在具有列限制的搜尋結果中排序直欄時，會在資料網格中顯示的限制列內完成排序。 • 對於開啓時間序列圖表的分組搜尋，列限制僅適用於資料網格。 時間序列圖表中的**前 N 個**下拉清單仍然控制圖表中繪製時序圖的次數。

程序

1. 選擇下列其中一個選項：
   - 若要搜尋事件，按一下**日誌活動**標籤。
   - 若要搜尋流程，按一下**網路活動**標籤。
2. 從**搜尋**清單框中，選取**新搜尋**。
3. 若要選取之前已儲存的搜尋：
   a. 請選擇下列其中一個選項：從「可用的已儲存搜尋」清單中，選取要載入的已儲存搜尋。 在「鍵入已儲存的搜尋或從清單選取」欄位中，鍵入要載入的搜尋名稱。
   b. 按一下**載入**。
   c. 在「編輯搜尋」窗格中，選取此搜尋使用的選項。 請參閱表 1。
4. 若要建立搜尋，請在「時間範圍」窗格內，選取要針對此搜尋擷取的時間範圍的選項。
5. 選用項目。 在「資料累積」窗格中，啓用唯一計數：
   a. 按一下**啓用唯一計數**。
   b. 在「警告」視窗中，讀取警告訊息，然後按一下**繼續**。 如需啓用唯一計數的相關資訊，請參閱表 1。
6. 在「搜尋參數」窗格中，定義您的搜尋準則：
   a. 從第一個清單框中，選取要搜尋的參數。 例如，裝置、來源埠或事件名稱。
   b. 從第二個清單框中，選取您要用於搜尋的修飾元。
   c. 在輸入欄位中，鍵入與您的搜尋參數相關的特定資訊。
   d. 按一下**新增過濾器**。
   e. 對於要新增至搜尋準則的每一個過濾器，重複步驟 a 到 d。
7. 選用項目。 若要在搜尋完成時自動儲存搜尋結果，請選取**搜尋完成時儲存結果**勾選框，然後鍵入已儲存的搜尋的名稱。
8. 在「直欄定義」窗格中，定義用於檢視結果的直欄和直欄佈置：
   a. 從**顯示**清單框中，選取設定爲與此搜尋相關聯的預先配置的直欄。
   b. 按一下**進階視圖定義**旁的箭頭，以顯示進階搜尋參數。

c. 自訂直欄，以顯示在搜尋結果內。請參閱表 1。

d. 選用項目。 在**結果限制**欄位中，鍵入要搜尋返回的列數。

9. 按一下**過濾器**。

結果

進行中（已完成 <percent>%）狀態會顯示在右上角。

.

在檢視局部搜尋結果時，搜尋引擎在背景中工作以完成搜尋，然後重新整理局部結果以更新視圖。

當搜尋完成時，在右上角會顯示**已完成**狀態。

儲存搜尋準則

您可以儲存配置的搜尋準則，以便可以重複使用該準則，並在其他元件（例如，報告）中使用已儲存的搜尋準則。 已儲存的搜尋準則不會到期。

關於這項作業

如果您指定搜尋的時間範圍，則搜尋名稱後面會附加指定的時間範圍。 例如，時間範圍爲前 5 分鐘的已儲存搜尋 Exploits by Source 會變成 Exploits by Source - Last 5 minutes。

如果您在先前儲存的搜尋中變更直欄集，然後使用相同的名稱儲存搜尋準則，則先前累積的時間序列圖表會遺失。

程序

1. 選擇下列其中一個選項：
   - 按一下**日誌活動**標籤。
   - 按一下**網路活動**標籤。
2. 執行搜尋。
3. 按一下**儲存準則**。
4. 輸入參數的值：

選項	敘述
參數	說明
搜尋名稱	鍵入要指派給這個搜尋準則的唯一名稱。
將搜尋指派給群組	請選取要指派這個已儲存的搜尋的群組的勾選框。 如果不選取群組，則會依預設將這個已儲存的搜尋指派給「其他」群組。 如需相關資訊，請參閱管理搜尋群組。
管理群組	按一下**管理群組**來管理搜尋群組。 如需相關資訊，請參閱管理搜尋群組。

選項	敘述
時間範圍選項：	選擇下列其中一個選項： • **即時（串流）** - 選取此選項以在處於串流模式時過濾搜尋結果。 • **前次間隔（自動重新整理）** - 選取此選項以在處於自動重新整理模式時過濾搜尋結果。**日誌活動**及**網路活動**標籤會以一分鐘間隔重新整理以顯示最近資訊。 • **最近** - 選取此選項，然後從這個清單框中選取要過濾的時間範圍。 • **特定間隔** - 選取此選項，然後從行事曆中選取要過濾的日期和時間範圍。
包含在我的快速搜尋中	選取此勾選框以在工具列上的**快速搜尋**清單框中包含此搜尋。
包含在我的儀表板中	選取此勾選框以在**儀表板**標籤上包含已儲存的搜尋資料。 如需**儀表板**標籤的相關資訊，請參閱儀表板管理。 **註**：僅當對搜尋進行分組時才會顯示這個參數。
設為預設值	選取此勾選框來將此搜尋設定爲預設的搜尋。
與每個人共用	選取此勾選框來與所有使用者共用這些搜尋需求。

5. 按一下**確定**。

排程搜尋

使用排程搜尋選項可排定搜尋及檢視結果。

您可以排定於白天或晚上的特定時間執行搜尋。

範例：
如果排定於晚上執行搜尋，則可以在白天調查結果。 與報告不同，您可以選擇分組搜尋結果以及進一步調查。 您可以搜尋網路群組中的多次失敗登入。 如果結果一般爲 10 個，而搜尋結果爲 100 個，則您可以分組搜尋結果，以方便調查。若要查看具有最多次失敗登入的使用者，您可以依使用者名稱進行分組。 您可以繼續進一步調查。

您可以透過**報告**標籤排定搜尋事件或流程。您必須對排程選取之前已儲存的搜尋準則集。

1. 建立報告

   在**報告精靈**視窗中指定下列資訊：
   - 圖表類型爲事件/日誌或流程。
   - 報告基於已儲存的搜尋。
   - 產生攻擊。

     您可以選擇**建立個別攻擊**選項或**新增結果至現有攻擊**選項。

     您還可以產生手動搜尋。

2. 檢視搜尋結果

您可以從**攻擊**標籤檢視排程搜尋的結果。

- 排程搜尋依**攻擊類性**欄識別。

  如果您要建立個別攻擊，則會在每次執行報告時產生攻擊。 如果要將儲存的搜尋結果新增至現有攻擊，則會在第一次執行報告時建立攻擊。 後續報告執行將會增添到此攻擊內。 如果沒有返回任何結果，則系統不會增添或建立攻擊。
- 若要在「攻擊摘要」視窗中檢視最近的搜尋結果，請按兩下攻擊清單中的排程搜尋結果。 若要檢視所有排程搜尋執行的清單，請在**最近 5 次搜尋結果**窗格中按一下**搜尋結果**。

您可以向使用者指派排定的搜尋攻擊。

相關工作:

第 129 頁的『搜尋符合準則的項目』
您可以搜尋符合搜尋準則的資料。

第 37 頁的『將攻擊指派給使用者』
使用**攻擊**標籤，您可以將攻擊指派給使用者以進行調查。

進階搜尋選項

使用**進階搜尋**欄位來輸入 Ariel 查詢語言 (AQL)，以指定所需的欄位以及如何對這些欄位進行分組來執行查詢。

進階搜尋欄位具有自動填寫及語法強調顯示功能。

使用自動填寫和語法強調顯示功能來協助建立查詢。如需受支援的 Web 瀏覽器的相關資訊，請參閱第 6 頁的『支援的 Web 瀏覽器』

存取進階搜尋

從**網路活動**和**日誌活動**標籤上的**搜尋**工具列中存取**進階搜尋**選項以輸入 AQL 查詢。

從**搜尋**工具列上的清單框中選取**進階搜尋**。

遵循下列步驟展開**進階搜尋**欄位：

1. 拖曳位於欄位右側的展開圖示。
2. 按 Shift + Enter 跳至下一行。
3. 按 Enter。

您可以用滑鼠右鍵按一下搜尋結果中的任何值，以按該值過濾。

按兩下搜尋結果中的任何列以查看更多詳細資料。

所有搜尋（包括 AQL 搜尋）均包括在審核日誌中。

AQL 搜尋字串範例

下表提供 AQL 搜尋字串的範例。

表 39. AQL 搜尋字串範例

說明	範例

從事件中選取預設直欄。
 	
從流程中選取預設直欄。
	`SELECT * FROM events`
	
	`SELECT * FROM flows`

選取特定直欄。	`SELECT sourceip, destinationip FROM events`
選取特定直欄並對結果進行排序。	`SELECT sourceip, destinationip FROM events ORDER BY destinationip`
執行聚集的搜尋查詢。	`SELECT sourceip, SUM(magnitude) AS magsum FROM events GROUP BY sourceip`
在 SELECT 子句中執行函數呼叫。	`SELECT CATEGORYNAME(category) AS namedCategory FROM events`
使用 WHERE 子句過濾搜尋結果。	`SELECT CATEGORYNAME(category) AS namedCategory, magnitude FROM events WHERE magnitude > 1`
根據規則名稱或規則名稱中的部分文字，搜尋觸發特定規則的事件。	`SELECT LOGSOURCENAME(logsourceid), * from events where RULENAME(creeventlist) ILIKE '%suspicious%'`
透過將欄位名稱包括在雙引號中，參照包含特殊字元（例如算術字元或空格）。	`SELECT sourceip, destinationip, "+field/name+" FROM events WHERE "+field/name+" LIKE '%test%'`

下表提供 X-Force 之 AQL 搜尋字串的範例。

表 40. X-Force 之 AQL 搜尋字串的範例

說明	範例
比對具有信任值之 X-Force 種類檢查 IP 位址。	`select * from events where XFORCE_IP_CONFIDENCE('Spam',sourceip)>3`
搜尋與 URL 相關聯的 X-Force URL 種類。	`select url, XFORCE_URL_CATEGORY(url) as myCategories from events where XFORCE_URL_CATEGORY(url) IS NOT NULL`
擷取與 IP 相關聯的 X-Force IP 種類。	`select sourceip, XFORCE_IP_CATEGORY (sourceip) as IPcategories from events where XFORCE_IP_CATEGORY(sourceip) IS NOT NULL`

如需函數、搜尋欄位和運算子的相關資訊，請參閱 *Ariel Query Language guide*（《Ariel 查詢語言手冊》）。

AQL 搜尋字串範例

使用 Ariel 查詢語言 (AQL) 可從 Ariel 資料庫中的事件、流程和 表格中擷取特定欄位。

註：當您建置 AQL 查詢時，如果您從任何文件中複製包含單引號的文字，並將文字貼上至 IBM Security QRadar，則您的查詢將不會進行剖析。您可以使用暫行解決方法，將文字貼上至 QRadar，並重新輸入單引號，或者可以從 IBM Knowledge Center 複製並貼上文字。

報告帳戶使用情形

不同的使用者社群可具有不同的威脅及使用情形指示器。

使用參照資料來報告數個使用者內容，例如部門、位置或經理。

您可以使用外部參照資料。

下列查詢會從使用者的登入事件中傳回使用者的相關 meta 資料資訊。

```
SELECT
REFERENCETABLE('user_data','FullName',username) as 'Full Name',
REFERENCETABLE('user_data','Location',username) as 'Location',
REFERENCETABLE('user_data','Manager',username) as 'Manager',
UNIQUECOUNT(username) as 'Userid Count',
UNIQUECOUNT(sourceip) as 'Source IP Count',
COUNT(*) as 'Event Count'
FROM events
WHERE qidname(qid) ILIKE '%logon%'
GROUP BY 'Full Name', 'Location', 'Manager'
LAST 1 days
```

多個帳戶 ID 之間的深入資訊

在此範例中，個別使用者在網路上具有多個帳戶。 組織需要使用者活動的單一視圖。

使用參照資料來將本端使用者 ID 對映至廣域 ID。

下列查詢會傳回在標示爲可疑的事件上，由廣域 ID 使用的使用者帳戶。

```
SELECT
REFERENCEMAP('GlobalID Mapping',username) as 'Global ID',
REFERENCETABLE('user_data','FullName', 'Global ID') as 'Full Name',
UNIQUECOUNT(username),
COUNT(*) as 'Event count'
FROM events
WHERE RULENAME(creEventlist) ILIKE '%suspicious%'
GROUP BY 'Global ID'
LAST 1 days
```

下列查詢顯示由廣域 ID 完成的活動。

```
SELECT
QIDNAME(qid) as 'Event name',
starttime as 'Time',
sourceip as 'Source IP', destinationip as 'Destination IP',
username as 'Event Username',
REFERENCEMAP('GlobalID_Mapping', username)as 'Global User'
FROM events
WHERE 'Global User' = 'John Doe'
LAST 1 days
```

識別可疑的長期引標

許多威脅使用指令和控制項來在數日、數週和數個月一次定期通訊。

進階搜尋可識別一段時間的連線型樣。 例如，您可以查詢 IP 位址之間每日/每週/每月一致、短期、低容體或連線數，或者是 IP 位址和地理位置。

使用 IBM Security QRadar REST API 來產生攻擊或者移入參照集或參照表格。

下列查詢偵測每小時引標的潛在實例。

```
SELECT sourceip, destinationip,
UNIQUECOUNT(DATEFORMAT(starttime,'hh')) as 'different hours',
COUNT(*) as 'total flows'
FROM flows
WHERE flowdirection = 'L2R'
GROUP BY sourceip, destinationip
HAVING 'different hours' > 20
AND 'total flows' < 25
LAST 24 hours
```

提示：您可以修改此查詢以處理 Proxy 日誌及其他事件類型。

下列查詢偵測每日引標的潛在實例。

```
SELECT sourceip, destinationip,
UNIQUECOUNT(DATEFORMAT(starttime,'dd'))as 'different days',
COUNT(*) as 'total flows'
FROM flows
WHERE flowdirection='L2R'
GROUP BY sourceip, destinationip
HAVING 'different days' > 4
AND 'total flows' < 14
LAST 7 days
```

下列查詢偵測來源 IP 與目的地 IP 之間的每日引標。 引標時間不是每日的相同時間。引標之間的時間延遲很短。

```
SELECT
sourceip,
DATEFORMAT(starttime,'hh') as hourofday,
(AVG( hourofday*hourofday) - (AVG(hourofday)^2))as variance,
COUNT(*) as 'total flows'
FROM flows
GROUP BY sourceip, destinationip
HAVING variance < 01 and 'total flows' < 10
LAST 7 days
```

下列查詢使用 Proxy 日誌事件來偵測網域的每日引標。 引標時間不是每日的相同時間。引標之間的時間延遲很短。

```
SELECT
sourceip,
DATEFORMAT(starttime,'hh') as hourofday,
(AVG(hourofday*hourofday) - (AVG(hourofday)^2)) as variance,
COUNT(*) as 'total events'
FROM events
WHERE LOGSOURCEGROUPNAME(devicegrouplist) ILIKE '%proxy%'
GROUP BY url_domain
HAVING variance < 0.1 and 'total events' < 10
LAST 7 days
```

url_domain 內容是 Proxy 日誌中的自訂內容。

外部威脅智能

與外部威脅智能資料相關的使用情形可提供重要事的威脅指示器。

進階搜尋可交互參照含有其他安全事件的外部威脅智能指示器及使用情形資料。

此查詢顯示您可以如何側寫許多日、週或月的外部威脅資料，以識別資產和帳戶的風險層次並設定優先順序。

```
Select
REFERENCETABLE('ip_threat_data','Category',destinationip) as 'Category',
REFERENCETABLE('ip_threat_data','Rating', destinationip) as 'Threat Rating',
UNIQUECOUNT(sourceip) as 'Source IP Count',
UNIQUECOUNT(destinationip) as 'Destination IP Count'
FROM events
GROUP BY 'Category', 'Threat Rating'
LAST 1 days
```

資產智慧與配置

威脅及使用情形指示器因資產類型、作業系統、漏洞狀態、伺服器類型、分類及其他參數而異。

在此查詢中，進階搜尋和資產模型提供位置的營運深入資訊。

Assetproperty 函數從資產擷取內容值，這可讓您將資產資料包括在結果中。

```
SELECT
ASSETPROPERTY('Location',sourceip) as location,
COUNT(*) as 'event count'
FROM events
GROUP BY location
LAST 1 days
```

下列查詢顯示您可以如何在資產模型中使用進階搜尋及使用者身分追蹤。

AssetUser 函數從資產資料庫擷取使用者名稱。

```
SELECT
APPLICATIONNAME(applicationid) as App,
ASSETUSER(sourceip, now()) as srcAssetUser,
COUNT(*) as 'Total Flows'
FROM flows
WHERE srcAssetUser IS NOT NULL
GROUP BY App, srcAssetUser
ORDER BY 'Total Flows' DESC
LAST 3 HOURS
```

Network LOOKUP 函數

您可以使用 **Network LOOKUP** 函數來擷取與 IP 位址相關聯的網路名稱。

```
SELECT NETWORKNAME(sourceip) as srcnet,
NETWORKNAME(destinationip) as dstnet
FROM events
```

Rule LOOKUP 函數

您可以使用 **Rule LOOKUP** 函數來透過規則的 ID 擷取規則的名稱。

```
SELECT RULENAME(123) FROM events
```

下列查詢會傳回觸發特定規則名稱的事件。

```
SELECT * FROM events
WHERE RULENAME(creEventList) ILIKE '%my rule name%'
```

全文檢索

您可以透過**進階搜尋**選項，使用 TEXT SEARCH 運算子來執行全文檢索。

在此範例中，有多個事件的內容裡包含單字 ″firewall″。 您可以使用**快速過濾器**選項，以及**日誌活動**標籤上的**進階搜尋**選項來搜尋這些事件。

- 若要使用**快速過濾器**選項，請於**快速過濾器**方框中鍵入下列文字：'firewall'
- 若要使用**進階搜尋**選項，請於**進階搜尋**方框中鍵入下列查詢：

  ```
  SELECT QIDNAME(qid) AS EventName, * from events where TEXT SEARCH 'firewall'
  ```

自訂內容

當您使用**進階搜尋**選項時，可以存取事件與流程的自訂內容。

下列查詢使用自訂內容 ″MyWebsiteUrl″ 來依據特定的 Web URL 排序事件：

```
SELECT "MyWebsiteUrl", * FROM events ORDER BY "MyWebsiteUrl"
```

相關概念:

『「快速過濾器」搜尋選項』
透過輸入使用簡式字詞或片語的文字搜尋字串來搜尋事件和流程有效負載。

相關工作:

第 158 頁的『建立 Regex 型自訂內容』
您可以建立 Regex 型自訂內容，以將事件或流程有效負載與正規表示式相符。

「快速過濾器」搜尋選項

透過輸入使用簡式字詞或片語的文字搜尋字串來搜尋事件和流程有效負載。

您可以從下列位置過濾搜尋：

日誌活動工具列及網路活動工具列

從**搜尋**工具列上的清單框中選取**快速過濾器**以輸入文字搜尋字串。按一下**快速過濾器**圖示以將**快速過濾器**套用至事件或流程清單。

新增過濾器對話框

按一下**日誌活動**或**網路活動**標籤上的**新增過濾器**圖示。

選取**快速過濾器**作爲過濾器參數，然後輸入文字搜尋字串。

流程搜尋頁面

將快速過濾器新增至過濾器清單。

當您在即時（串流）或前次間隔模式下檢視**流程**時，您只能在**快速過濾器**欄位中輸入簡式字詞或片語。當您檢視某個時間範圍內的**事件** 或**流程**時，請遵循下列語法準則：

表 41. 快速過濾器語法準則

說明	範例
包含您預期在有效負載中尋找的所有純文字。	`Firewall`
透過將多個搜尋詞彙包括在雙引號中，搜尋片語全文。	`"Firewall deny"`

表 41. 快速過濾器語法準則 (繼續)

說明	範例
包含單一及多個萬用字元。搜尋詞彙不能以萬用字元開頭。	`F?rewall 或 F??ew*`
使用邏輯表示式將詞彙分組，如 AND、OR 及 NOT。 爲了識別爲邏輯表示式而不是搜尋詞彙，語法和運算子必須大寫。	`(%PIX* AND ("Accessed URL" OR "Deny udp src") AND 10.100.100.*)`
建立包含 NOT 邏輯表示式的搜尋準則時，您必須包含至少一個其他邏輯表示式類型，否則，不會傳回任何結果。	`(%PIX* AND ("Accessed URL" OR "Deny udp src") NOT 10.100.100.*)`
下列字元前面必須加反斜線，以指出該字元是搜尋詞彙的一部分：`+ - && || ! () {} [] ^ " ~ * ? : \.`	`"%PIX\-5\-304001"`

依序從有效負載單字或片語中的第一個字元起符合搜尋詞彙。 搜尋詞彙 `user` 符合 `user_1` 及 `user_2`，但不符合下列片語：`ruser`、`myuser` 或 `anyuser`。

「快速過濾器」搜尋使用英文語言環境。 *語言環境*是識別語言或地理位置，以及判定格式化使用慣例（例如，對照、大小寫轉換、字元分類、訊息的語言、日期和時間表示法，以及數字表示法）的設定。

語言環境是由作業系統設定的。 您可以將 QRadar 配置爲置換作業系統的語言環境設定。 例如，您可以將語言環境設定爲**英文**，而 QRadar 主控台 可以設定爲 **Italiano**（**義大利文**）。

如果您在「快速過濾器」搜尋查詢中使用 Unicode 字元，則可能返回非預期的搜尋結果。

如果您選擇非英文語言環境，則可以在 QRadar 中使用進階搜尋選項來搜尋事件和有效負載資料。

相關概念:

第 129 頁的第 9 章, 『資料搜尋』
在**日誌活動**、**網路活動**及**攻擊**標籤上，您可以使用特定的準則搜尋事件、流程及攻擊。

第 135 頁的『進階搜尋選項』
使用**進階搜尋**欄位來輸入 Ariel 查詢語言 (AQL)，以指定所需的欄位以及如何對這些欄位進行分組來執行查詢。

第 136 頁的『AQL 搜尋字串範例』
使用 Ariel 查詢語言 (AQL) 可從 Ariel 資料庫中的事件、流程和 表格中擷取特定欄位。

相關工作:

第 15 頁的『更新使用者喜好設定』
您可以設定 IBM Security QRadar SIEM 使用者介面中的使用者喜好設定，例如，語言環境。

攻擊搜尋

搜尋攻擊的方法是，使用特定準則來顯示符合結果清單中的搜尋準則的攻擊。

您可以建立新搜尋或載入先前儲存的一組搜尋準則。

在「我的攻擊」和「所有攻擊」頁面上搜尋攻擊

您可以在**攻擊**標籤的「我的攻擊」和「所有攻擊」頁面上搜尋符合準則的攻擊。

關於這項作業

下表說明在**我的攻擊**和**所有攻擊**頁面上可以用來搜尋攻擊資料的搜尋選項。

如需種類的相關資訊，請參閱 *IBM Security QRadar SIEM Administration Guide*。

表 42. 「我的攻擊」和「所有攻擊」頁面搜尋選項

選項	說明
分組	此清單框容許您在**可用的已儲存搜尋**清單中選取要「搜尋群組」檢視的攻擊。
鍵入已儲存的搜尋或從清單選取	此欄位容許您鍵入已儲存的搜尋名稱或關鍵字，以過濾**可用的已儲存搜尋**清單。
可用的已儲存的搜尋	此清單會顯示所有可用的搜尋，除非您使用「分組或鍵入已儲存的搜尋」或「**從清單選取**」選項來向清單套用過濾器。 您可以選取這個清單上某個已儲存的搜尋來顯示或編輯。
所有攻擊	此選項容許您搜尋所有攻擊，而不論時間範圍。
最近	此選項容許您選取預先定義的時間範圍來過濾。 選取此選項之後，必須從清單框選取一個時間範圍選項。
特定間隔	此選項容許您配置搜尋自訂時間範圍。 選取此選項之後，必須選取下列其中一項。 • **開始日期介於** - 選取此勾選框來搜尋特定時段期間開始的攻擊。選取此勾選框之後，使用清單框來選取要搜尋的日期。 • **最後一個事件/流程介於** - 選取此勾選框來搜尋在特定時段內發生最後一個偵測事件的攻擊。選取此勾選框之後，使用清單框來選取要搜尋的日期。
搜尋	**搜尋**圖示在搜尋頁面上的多個窗格內提供。 您可以在完成配置搜尋並希望檢視結果時按一下**搜尋**。
攻擊 ID	在這個欄位中，您可以鍵入要搜尋的「攻擊 ID」。
說明	在這個欄位中，您可以鍵入要搜尋的說明。
已指派給使用者	從這個清單框中，您可以選取要搜尋的使用者名稱。

表 42. 「我的攻擊」和「所有攻擊」頁面搜尋選項 (繼續)

選項	說明
方向	從這個清單框中，您可以選取要搜尋的攻擊方向。 選項包括： • 本端到本端 • 本端到遠端 • 遠端到本端 • 遠端到遠端 • 本端到遠端或本端 • 遠端到遠端或本端
來源 IP	在這個欄位中，您可以鍵入要搜尋的來源 IP 位址或 CIDR 範圍。
目的地 IP	在這個欄位中，您可以鍵入要搜尋的目的地 IP 位址或 CIDR 範圍。
長度	從這個清單框中，可以指定長度，然後選取只顯示長度等於、小於或大於配置值的攻擊。 範圍爲 0 - 10。
嚴重性	從這個清單框中，可以指定嚴重性，然後選取只顯示嚴重性等於、小於或大於配置值的攻擊。 範圍爲 0 - 10。
可靠性	從這個清單框中，可以指定可靠性，然後選取只顯示可靠性等於、小於或大於配置值的攻擊。 範圍爲 0 - 10。
相關性	從這個清單框中，可以指定相關性，然後選取只顯示相關性等於、小於或大於配置值的攻擊。 範圍爲 0 - 10。
包含使用者名稱	在這個欄位中，您可以鍵入正規表示式 (Regex) 陳述式，以搜尋包含特定使用者名稱的攻擊。當您定義自訂正規表示式型樣時，請遵守 Java™ 程式設計語言定義的正規表示式規則。 如需相關資訊，可以參閱 Web 上的 Regex 指導教學。
來源網路	從這個清單框中，您可以選取要搜尋的來源網路。
目的地網路	從這個清單框中，您可以選取要搜尋的目的地網路。
高階種類	從這個清單框中，您可以選取要搜尋的高階種類。.
低階種類	從這個清單框中，您可以選取要搜尋的低階種類。

表 42. 「我的攻擊」和「所有攻擊」頁面搜尋選項 (繼續)

選項	說明
排除	這個窗格中的選項容許您從搜尋結果中排除攻擊。 選項包括： • 作用中的攻擊 • 隱藏的攻擊 • 已關閉的攻擊 • 非作用中的攻擊 • 受保護的攻擊
由使用者關閉	僅當「排除」窗格中清除了**已關閉攻擊**勾選框時才會顯示此參數。 從這個清單框中，您可以選取要針對其搜尋已關閉的攻擊的使用者名稱，或選取**全部**以顯示所有已關閉的攻擊。
關閉原因	僅當「排除」窗格中清除了**已關閉攻擊**勾選框時才會顯示此參數。 從這個清單框中，您可以選取要針對其搜尋已關閉的攻擊的原因，或選取**全部**以顯示所有已關閉的攻擊。
事件	從這個清單框中，可以指定事件計數，然後選取只顯示事件計數等於、小於或大於配置值的攻擊。
流程	從這個清單框中，可以指定流程計數，然後選取只顯示流程計數等於、小於或大於配置值的攻擊。
事件/流程總計	從這個清單框中，可以指定事件及流程總數，然後選取只顯示事件及流程總數等於、小於或大於配置值的攻擊。
目的地	從這個清單框中，可以指定目的地 IP 位址計數，然後選取只顯示目的地 IP 位址計數等於、小於或大於配置值的攻擊。
日誌來源群組	從這個清單框中，您可以選取包含要搜尋之日誌來源的日誌來源群組。 **日誌來源**清單框會顯示指派給選取的日誌來源群組的所有日誌來源。
日誌來源	從這個清單框中，您可以選取要搜尋的日誌來源。
規則群組	從這個清單框中，您可以選取包含要搜尋之提出規則的規則群組。 **規則**清單框會顯示指派給選取的規則群組的所有規則。
規則	從這個清單框中，您可以選取要搜尋的提出規則。
攻擊類型	從這個清單框中，您可以選取要搜尋的攻擊類型。 如需**攻擊類型**清單框中各選項的相關資訊，請參閱表 2。

下表說明了**攻擊類型**清單框中可用的選項：

表 43. 攻擊類型選項

攻擊類型	說明
任何	此選項會搜尋所有攻擊來源。
來源 IP	若要搜尋具有特定來源 IP 位址的攻擊，您可以選取此選項，然後鍵入要搜尋的來源 IP 位址。
目的地 IP	若要搜尋具有特定目的地 IP 位址的攻擊，您可以選取此選項，然後鍵入要搜尋的目的地 IP 位址。
事件名稱	若要搜尋具有特定事件名稱的攻擊，您可以按一下**瀏覽**圖示來開啓「事件瀏覽器」，並選取要搜尋的事件名稱 (QID)。 您可以使用下列其中一項搜尋特定的 QID： • 若要依種類搜尋 QID，請選取**依種類瀏覽**勾選框，然後從清單框中選取高階或低階種類。 • 若要依日誌來源類型搜尋 QID，請從**日誌來源類型**清單框選取**依日誌來源類型瀏覽**勾選框。 • 若要依日誌來源類型搜尋 QID，請從**日誌來源類型**清單框選取**依日誌來源類型瀏覽**勾選框。 • 若要依名稱搜尋 QID，請選取 **QID 搜尋**勾選框，然後在 **QID/名稱**欄位中鍵入名稱。
使用者名稱	若要搜尋具有特定使用者名稱的攻擊，您可以選取此選項，然後鍵入要搜尋的使用者名稱。
來源 MAC 位址	若要搜尋具有特定來源 MAC 位址的攻擊，您可以選取此選項，然後鍵入要搜尋的來源 MAC 位址。
目的地 MAC 位址	若要搜尋具有特定目的地 MAC 位址的攻擊，您可以選取此選項，然後鍵入要搜尋的目的地 MAC 位址。
日誌來源	從**日誌來源群組**清單框中，您可以選取包含要搜尋之日誌來源的日誌來源群組。 **日誌來源**清單框會顯示指派給選取的日誌來源群組的所有日誌來源。 從**日誌來源**清單框中，您可以選取要搜尋的日誌來源。
主機名稱	若要搜尋具有特定主機名稱的攻擊，您可以選取此選項，然後鍵入要搜尋的主機名稱。
來源埠	若要搜尋具有特定來源埠的攻擊，您可以選取此選項，然後鍵入要搜尋的來源埠。
目的地埠	若要搜尋具有特定目的地埠的攻擊，您可以選取此選項，然後鍵入要搜尋的目的地埠。

表 43. 攻擊類型選項 (繼續)

攻擊類型	說明
來源 IPv6	若要搜尋具有特定來源 IPv6 位址的攻擊，您可以選取此選項，然後鍵入要搜尋的來源 IPv6 位址。
目的地 IPv6	若要搜尋具有特定目的地 IPv6 位址的攻擊，您可以選取此選項，然後鍵入要搜尋的目的地 IPv6 位址。
來源 ASN	若要搜尋具有特定來源 ASN 的攻擊，您可以從**來源 ASN** 清單框選取來源 ASN。
目的地 ASN	若要搜尋具有特定目的地 ASN 的攻擊，您可以從**目的地 ASN** 清單框選取目的地 ASN。
規則	若要搜尋與特定規則相關聯的攻擊，您可以從**規則群組**清單框中，選取包含要搜尋之規則的規則群組。 **規則群組**清單框會顯示指派給選取的規則群組的所有規則。 從**規則**清單框中，您可以選取要搜尋的規則。
應用程式 ID	若要搜尋具有特定應用程式 ID 的攻擊，您可以從**應用程式 ID** 清單框選取應用程式 ID。

程序

1. 按一下**攻擊**標籤。
2. 從**搜尋**清單框中，選取**新搜尋**。
3. 選擇下列其中一個選項：
   - 若要載入之前儲存的搜尋，請跳至第 4 步。
   - 若要建立新搜尋，請跳至第 7 步。
4. 使用下列其中一項來選取之前儲存的搜尋：
   - 從**可用的已儲存搜尋**清單，選取要載入的已儲存搜尋。
   - 在**鍵入已儲存的搜尋**或**從清單選取**欄位中，鍵入要載入的搜尋名稱。
5. 按一下**載入**。
6. 選用項目。 在「編輯搜尋」窗格中選取**設為預設值**勾選框，以將此搜尋設定爲您的預設搜尋。如果將此搜尋設定爲您的預設搜尋，則會在您每次存取**攻擊**標籤時自動執行該搜尋，並顯示結果。
7. 在「時間範圍」窗格上，選取要針對此搜尋擷取的時間範圍的選項。 請參閱表 1。
8. 在「搜尋參數」窗格中，定義特定搜尋準則。 請參閱表 1。
9. 在「攻擊來源」窗格中，指定要搜尋的攻擊類型與攻擊來源：
   a. 從清單框中，選取要搜尋的攻擊類型。
   b. 鍵入搜尋參數。 請參閱表 2。
10. 在「直欄定義」窗格中，定義結果的排序順序：
    a. 從第一個清單框中，選取要作爲搜尋結果排序依據的直欄。
    b. 從第二個清單框中，選取搜尋結果的顯示順序。 選項包括降冪與升冪。
11. 按一下**搜尋**。

下一步

儲存「攻擊」標籤上的搜尋準則

在「依來源 IP」頁上搜尋攻擊

此主題提供了如何在**攻擊**標籤的**依來源 IP** 頁上搜尋攻擊的程序。

關於這項作業

下表說明了在「依來源 IP」頁面上搜尋攻擊資料可以使用的搜尋選項：

表 44. 「依來源 IP」頁面搜尋選項

選項	說明
所有攻擊	您可以選取此選項來搜尋所有來源 IP 位址，而不論時間範圍。
最近	您可以選取此選項，然後從這個清單框中選取要搜尋的時間範圍。
特定的間隔	若要指定搜尋間隔，可以選取「特定間隔」選項，然後選取下列一項： • **開始日期介於** - 選取此勾選框來搜尋與特定時段期間開始的攻擊相關聯的來源 IP 位址。選取此勾選框之後，使用清單框來選取要搜尋的日期。 • **最後一個事件/流程介於** - 選取此勾選框來搜尋與在特定時段內發生最後一個偵測事件的攻擊相關聯的來源 IP 位址。選取此勾選框之後，使用清單框來選取要搜尋的日期。
搜尋	**搜尋**圖示在搜尋頁面上的多個窗格內提供。 您可以在完成配置搜尋並希望檢視結果時按一下**搜尋**。
來源 IP	在這個欄位中，您可以鍵入要搜尋的來源 IP 位址或 CIDR 範圍。
長度	從這個清單框中，可以指定長度，然後選取只顯示長度等於、小於或大於配置值的攻擊。 範圍爲 0 - 10。
VA 風險	從這個清單框中，可以指定 VA 風險，然後選取只顯示 VA 風險等於、小於或大於配置值的攻擊。 範圍爲 0 - 10。
事件/流程	從這個清單框中，可以指定事件或流程計數，然後選取只顯示長度等於、小於或大於配置值的攻擊。
排除	您可以選取要從搜尋結果中排除的攻擊的勾選框。 選項包括： • **作用中的攻擊** • **隱藏的攻擊** • **已關閉的攻擊** • **非作用中的攻擊** • **受保護的攻擊**

表 44. 「依來源 IP」頁面搜尋選項 (繼續)

選項	說明

程序

1. 按一下**攻擊**標籤。
2. 按一下**依來源 IP**。
3. 從**搜尋**清單框中，選取**新搜尋**。
4. 在「時間範圍」窗格上，選取要針對此搜尋擷取的時間範圍的選項。 請參閱表 1。
5. 在「搜尋參數」窗格中，定義特定搜尋準則。 請參閱表 1。
6. 在「直欄定義」窗格中，定義結果的排序順序：
   a. 從第一個清單框中，選取要作爲搜尋結果排序依據的直欄。
   b. 從第二個清單框中，選取搜尋結果的顯示順序。 選項包括**降冪**和**升冪**。
7. 按一下**搜尋**。

下一步

儲存「攻擊」標籤上的搜尋準則

在「依目的地 IP」頁上搜尋攻擊

在**攻擊**標籤的**「依目的地 IP」**頁上，您可以搜尋依目的地 IP 位址分組的攻擊。

關於這項作業

下表說明了在「依目的地 IP」頁面上搜尋攻擊可以使用的搜尋選項：

表 45. 「依目的地 IP」頁面搜尋選項

選項	說明
所有攻擊	您可以選取此選項來搜尋所有目的地 IP 位址，而不論時間範圍。
最近	您可以選取此選項，然後從這個清單框中選取要搜尋的時間範圍。
特定間隔	若要指定特定搜尋間隔，可以選取**特定間隔**選項，然後選取下列一項： • 若要指定特定搜尋間隔，可以選取**特定間隔**選項，然後選取下列一項： • **最後一個事件/流程介於** - 選取此勾選框來搜尋與在特定時段內發生最後一個偵測事件的攻擊相關聯的目的地 IP 位址。選取此勾選框之後，使用清單框來選取要搜尋的日期。
搜尋	**搜尋**圖示在搜尋頁面上的多個窗格內提供。 您可以在完成配置搜尋並希望檢視結果時按一下**搜尋**。
目的地 IP	您可以鍵入要搜尋的目的地 IP 位址或 CIDR 範圍。

表 45. 「依目的地 IP」頁面搜尋選項 (繼續)

選項	說明
長度	從這個清單框中，可以指定長度，然後選取只顯示長度等於、小於或大於配置值的攻擊。
VA 風險	從這個清單框中，可以指定 VA 風險，然後選取只顯示 VA 風險等於、小於或大於配置值的攻擊。 範圍爲 0 - 10。
事件/流程	從這個清單框中，可以指定事件或流程計數長度，然後選取只顯示事件或流程計數等於、小於或大於配置值的攻擊。

程序

1. 按一下**攻擊**標籤。
2. 在導覽功能表上，按一下**依目的地 IP**。
3. 從**搜尋**清單框中，選取**新搜尋**。
4. 在「時間範圍」窗格上，選取要針對此搜尋擷取的時間範圍的選項。 請參閱表 1。
5. 在「搜尋參數」窗格中，定義特定搜尋準則。 請參閱表 1。
6. 在「直欄定義」窗格中，定義結果的排序順序：
   a. 從第一個清單框中，選取要作爲搜尋結果排序依據的直欄。
   b. 從第二個清單框中，選取搜尋結果的顯示順序。 選項包括**降冪**和**升冪**。
7. 按一下**搜尋**。

下一步

儲存「攻擊」標籤上的搜尋準則

在「依網路」頁上搜尋攻擊

在**攻擊**標籤的**「依網路」**頁上，您可以搜尋依關聯網路分組的攻擊。

關於這項作業

下表說明了在「依網路」頁面上搜尋攻擊資料可以使用的搜尋選項：

表 46. 在「依網路」頁面上搜尋攻擊資料的搜尋選項

選項	說明
網路	從這個清單框中，您可以選取要搜尋的網路。
長度	從這個清單框中，可以指定長度，然後選取只顯示長度等於、小於或大於配置值的攻擊。
VA 風險	從這個清單框中，可以指定 VA 風險，然後選取只顯示 VA 風險等於、小於或大於配置值的攻擊。
事件/流程	從這個清單框中，可以指定事件或流程計數，然後選取只顯示事件或流程計數等於、小於或大於配置值的攻擊。

程序

1. 按一下**攻擊**標籤。
2. 按一下**依網路**。
3. 從**搜尋**清單框中，選取**新搜尋**。
4. 在「搜尋參數」窗格中，定義特定搜尋準則。 請參閱表 1。
5. 在「直欄定義」窗格中，定義結果的排序順序：
   a. 從第一個清單框中，選取要作爲搜尋結果排序依據的直欄。
   b. 從第二個清單框中，選取搜尋結果的顯示順序。 選項包括**降冪**和**升冪**。
6. 按一下**搜尋**。

下一步

儲存「攻擊」標籤上的搜尋準則

儲存*攻擊*標籤上的搜尋準則

在**攻擊**標籤上，您可以儲存配置的搜尋準則，以便將來搜尋時重複使用該準則。 已儲存的搜尋準則不會到期。

程序

1. 程序
2. 執行搜尋。 請參閱攻擊搜尋。
3. 按一下**儲存準則**。
4. 輸入下列參數的值：

選項	敘述
參數	說明
搜尋名稱	鍵入要指派給這個搜尋準則的名稱。
管理群組	按一下**管理群組**來管理搜尋群組。 請參閱管理搜尋群組。
時間範圍選項：	選擇下列其中一個選項： • **所有攻擊** - 選取此選項以搜尋所有攻擊，而不論時間範圍。 • **最近** - 選取此選項，然後從這個清單框中選取要搜尋的時間範圍。 • **特定間隔** - 若要指定要搜尋的特定間隔，請選取**特定間隔**選項，然後選取下列一項：開始日期介於 - 選取此勾選框來搜尋特定時段期間開始的攻擊。 選取此勾選框之後，使用清單框來選取要搜尋的日期。 最後一個事件/流程介於 - 選取此勾選框來搜尋在特定時段內發生最後一個偵測事件的攻擊。選取此勾選框之後，使用清單框來選取要搜尋的日期。最後一個事件介於 - 選取此勾選框來搜尋在特定時段內發生最後一個偵測事件的攻擊。選取此勾選框之後，使用清單框來選取要搜尋的日期。

選項	敘述
設為預設值	選取此勾選框來將此搜尋設定爲預設的搜尋。

5. 按一下**確定**。

刪除搜尋準則

您可以刪除搜尋準則。

關於這項作業

在您刪除已儲存的搜尋時，則與已儲存的搜尋相關聯的物件可能無法運作。 報告及異常偵測規則是使用已儲存的搜尋準則的 QRadar 物件。 在您刪除已儲存的搜尋之後，編輯相關聯的物件以確保它們繼續運作。

程序

1. 選擇下列其中一個選項：
   - 按一下**日誌活動**標籤。
   - 按一下**網路活動**標籤。
2. 從**搜尋**清單框中，選取**新建搜尋**或**編輯搜尋**。
3. 在「已儲存的搜尋」窗格中，從**可用的已儲存的搜尋**清單框中選取已儲存的搜尋。
4. 按一下**刪除**。
   - 如果已儲存的搜尋準則與其他 QRadar 物件不關聯，畫面上會顯示確認視窗。
   - 如果已儲存的搜尋準則與其他物件不關聯，畫面上會顯示「刪除已儲存的搜尋」視窗。視窗會列出與您要刪除的已儲存搜尋相關聯的物件。 請記下相關聯的物件。
5. 按一下**確定**。
6. 選擇下列其中一個選項：
   - 按一下**確定**以繼續。
   - 按一下**取消**以關閉「刪除已儲存的搜尋」視窗。

下一步

如果已儲存的搜尋準則已與其他 QRadar 物件相關聯，請存取您記下的相關聯物件，並編輯物件以移除或取代與已刪除的已儲存搜尋的關聯。

使用子搜尋來細化搜尋結果

您可以使用子搜尋在已完成的一組搜尋結果內進行搜尋。 子搜尋用來細化搜尋結果，而不必重新搜尋資料庫。

開始之前

當您定義要作爲子搜尋基準的搜尋時，請確定已停用「即時（串流）」選項，且沒有對搜尋進行分組。

關於這項作業

此功能無法用於已分組的搜尋、進行中的搜尋或串流模式的搜尋。

程序

1. 選擇下列其中一個選項：
   - 按一下**日誌活動**標籤。
   - 按一下**網路活動**標籤。
2. 執行搜尋。
3. 當您的搜尋完成時，新增另一個過濾器：
   a. 按一下**新增過濾器**。
   b. 從第一個清單框中，選取要搜尋的參數。
   c. 從第二個清單框中，選取您要用於搜尋的修飾元。 可用的修飾元清單視您在第一個清單中選取的屬性而定。
   d. 在輸入欄位中，鍵入與您的搜尋相關的特定資訊。
   e. 按一下**新增過濾器**。

結果

「原始過濾器」窗格指定套用至基本搜尋的原始過濾器。 「現行過濾器」窗格指定套用至子搜尋的過濾器。 您可以清除子搜尋過濾器，而不必重新啓動基本搜尋。 按一下要清除之過濾器旁的**清除過濾器**鏈結。 如果從「原始過濾器」窗格清除過濾器，則會重新啓動基本搜尋。

如果刪除已儲存之子搜尋準則的基本搜尋準則，則您仍然可以存取已儲存的子搜尋準則。 如果新增過濾器，則子搜尋會搜尋整個資料庫，因爲搜尋功能不再將搜尋基於之前搜尋的資料集。

下一步

儲存搜尋準則

管理搜尋結果

您可以起始多個搜尋，然後在搜尋於背景中完成時，導覽至其他標籤來執行其他作業。

您可以將搜尋配置爲在搜尋完成時向您傳送電子郵件通知。

在搜尋進行時的任何時間，您都可以回到**日誌活動** 或**網路活動**標籤來檢視部分或完整的搜尋結果。

取消搜尋

搜尋已排入佇列或正在進行時，您可以在「管理搜尋結果」頁面上取消搜尋。

關於這項作業

如果您在搜尋正在進行時予以取消，在取消之前，累計的結果會保持不變。

程序

1. 選擇下列其中一個選項：
   - 按一下**日誌活動**標籤。
   - 按一下**網路活動**標籤。
2. 從**搜尋**功能表中，選取**管理搜尋結果**。
3. 選取您要取消的已排入佇列的或正在進行的搜尋結果。
4. 按一下**取消**。
5. 按一下**是**。

刪除搜尋

如果不再需要搜尋結果，您可以從「管理搜尋結果」頁面刪除搜尋結果。

程序

1. 選擇下列其中一個選項：
   - 按一下**日誌活動**標籤。
   - 按一下**網路活動**標籤。
2. 從**搜尋**功能表中，選取**管理搜尋結果**。
3. 選取您要刪除的搜尋結果。
4. 按一下**刪除**。
5. 按一下**是**。

管理搜尋群組

使用「搜尋群組」視窗，您可以建立及管理事件、流程及攻擊搜尋群組。

這些群組可讓您輕鬆地在**日誌活動**、**網路活動**及**攻擊**標籤上及「報告」精靈中尋找已儲存的搜尋準則。

檢視搜尋群組

可以使用預設的一組群組和子群組。

關於這項作業

您可以在「事件搜尋群組」、「流程搜尋群組」或「攻擊搜尋群組」視窗上檢視搜尋群組。

所有未指派給群組的已儲存搜尋位於**其他**群組內。

「事件搜尋群組」、「流程搜尋群組」及「攻擊搜尋群組」視窗顯示每一個群組的下列參數。

表 47. 「搜尋群組」視窗參數

參數	說明
名稱	指定搜尋群組的名稱。
使用者	指定建立搜尋群組的使用者的名稱。
說明	指定搜尋群組的說明。

表 47. 「搜尋群組」視窗參數 (繼續)

參數	說明
修改日期	指定搜尋群組的修改日期。

「事件搜尋群組」、「流程搜尋群組」及「攻擊搜尋群組」視窗工具列提供下列功能。

表 48. 「搜尋群組」視窗工具列功能

功能	說明
新增群組	若要建立新搜尋群組，可以按一下**新群組**。 請參閱建立新搜尋群組。
編輯	若要編輯現有搜尋群組，可以按一下**編輯**。請參閱編輯搜尋群組。
複製	若要將已儲存的搜尋複製到其他搜尋群組，可以按一下**複製**。 請參閱將已儲存的搜尋複製到其他群組。
移除	若要移除搜尋群組，或從搜尋群組移除已儲存的搜尋，請選取要移除的項目，然後按一下**移除**。 請參閱移除群組，或從群組移除已儲存的搜尋。

程序

1. 選擇下列其中一個選項：
   - 按一下**日誌活動**標籤。
   - 按一下**網路活動**標籤。
2. **選取搜尋 > 編輯搜尋**。
3. 按一下**管理群組**。
4. 檢視搜尋群組。

建立新的搜尋群組

您可以建立新的搜尋群組。

程序

1. 選擇下列其中一個選項：
   - 按一下**日誌活動**標籤。
   - 按一下**網路活動**標籤。
2. 選取**搜尋 編輯搜尋**。
3. 按一下**管理群組**。
4. 選取您要在其中建立新群組的群組的資料夾。
5. 按一下**新建群組**。
6. 在**名稱**欄位中，鍵入新群組的唯一名稱。
7. 選用項目。 在**說明**欄位中，鍵入說明。
8. 按一下**確定**。

編輯搜尋群組

您可以編輯搜尋群組的**名稱**及**說明**欄位。

程序

1. 選擇下列其中一個選項：
   - 按一下**日誌活動**標籤。
   - 按一下**網路活動**標籤。
2. 選取**搜尋 > 編輯搜尋**。
3. 按一下**管理群組**。
4. 選取您要編輯的群組。
5. 按一下**編輯**。
6. 編輯參數：
   - 在**名稱**欄位中鍵入新名稱。
   - 在**說明**欄位中鍵入新說明。
7. 按一下**確定**。

將已儲存的搜尋複製到其他群組

您可以將已儲存的搜尋複製到一個以上群組。

程序

1. 選擇下列其中一個選項：
   - 按一下**日誌活動**標籤。
   - 按一下**網路活動**標籤。
2. 選取**搜尋 > 編輯搜尋**。
3. 按一下**管理群組**。
4. 選取您要複製的已儲存的搜尋。
5. 按一下**複製**。
6. 在「項目群組」視窗上，選取您要複製已儲存的搜尋至其中的群組的勾選框。
7. 按一下**指派群組**。

移除群組或從群組移除已儲存的搜尋

您可以使用**移除**圖示從群組移除搜尋或移除搜尋群組。

關於這項作業

當您從群組移除已儲存的搜尋時，不會從系統刪除已儲存的搜尋。 已儲存的搜尋將從群組移除，並自動移至**其他**群組。

您無法從系統移除下列群組：

- 事件搜尋群組
- 流程搜尋群組
- 攻擊搜尋群組
- 其他

程序

1. 選擇下列其中一個選項：
   - 按一下**日誌活動**標籤。
   - 按一下**網路活動**標籤。
2. 選取**搜尋 > 編輯搜尋**。
3. 按一下**管理群組**。
4. 選擇下列其中一個選項：
   - 選取要從群組移除的已儲存的搜尋。
   - 選取您要移除的群組。
5. 按一下**移除**。
6. 按一下**確定**。

第 10 章 自訂事件和流程內容

使用自訂事件和流程內容可搜尋、檢視及報告在日誌內 QRadar 通常未正規化及顯示的資訊。

您可以從**日誌活動** 或**網路活動**標籤上的數個位置，建立自訂事件和流程內容：

- 從**日誌活動**標籤，按兩下事件，然後按一下**擷取內容**。
- 從**網路活動**標籤，按兩下流程，然後按一下**擷取內容**。
- 您可以從「搜尋」頁面建立或編輯自訂事件或流程內容。在您從「搜尋」頁面建立自訂內容時，不會從任何特定事件或流程衍生內容；因此，「自訂事件內容」視窗中不會預先移入內容。您可以從另一個來源複製並貼上有效負載資訊。

所需許可權

在您具有正確許可權時建立自訂內容。

您必須具有「使用者定義的事件內容」或「使用者定義的流程內容」許可權。

如果具有管理許可權，您也可以透過「管理」標籤建立及修改自訂內容。

按一下**管理** > **資料來源** > **自訂事件內容** > 或**管理** > **資料來源** > **自訂流程內容**。

請洽詢管理者，以確保您具有正確的許可權。

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

自訂內容類型

您可以建立自訂內容類型。

在您建立自訂內容時，可以選擇建立正規表示式或計算的內容類型。

使用正規表示式 (Regex) 陳述式，您可以從事件或流程有效負載擷取非正規化資料。

例如，建立報告以報告在 Oracle 伺服器上進行使用者許可權變更的所有使用者。 系統會報告使用者清單，及使用者對其他帳戶的許可權進行變更的次數。 但是，通常無法顯示實際使用者帳戶或已變更的許可權。 您可以建立自訂內容以從日誌擷取此資訊，然後在搜尋及報告中使用此內容。 使用此功能需要進一步瞭解正規表示式 (Regex)。

正規表示式定義您希望成爲自訂內容的欄位。輸入正規表示式陳述式之後，您可以根據有效負載對其進行驗證。 在您定義自訂正規表示式型樣時，請遵循 Java 程式設計語言定義的正規表示式規則。

如需相關資訊，您可以參閱 Web 上可用的正規表示式指導教學。 自訂內容可以與多個正規表示式相關聯。

在剖析事件或流程時，對事件或流程測試每個正規表示式型樣，直到正規表示式型樣與有效負載相符。與事件或流程有效負載相符的第一個正規表示式型樣可判定要擷取的資料。

使用計算型自訂內容，您可以對現有的數值事件或流程內容執行計算，以產生計算的內容。

例如，您可以建立一個內容，它透過將一個數值內容除以另一個數值內容來顯示百分比。

建立 Regex 型自訂內容

您可以建立 Regex 型自訂內容，以將事件或流程有效負載與正規表示式相符。

關於這項作業

在您配置 Regex 型自訂內容時，「自訂事件內容」或「自訂流程內容」視窗會提供參數。下表提供部分參數的參照資訊。

表 49. 「自訂事件內容」視窗參數 (Regex)

參數	說明
測試欄位	
新建內容	新的內容名稱不能是正規化內容的名稱，例如，使用者名稱、來源 IP 或目的地 IP。
最佳化規則、報告及搜尋的剖析	第一次接收到事件或流程時剖析與儲存內容。當您選取此勾選框時，內容不需要進一步剖析來產生報告、搜尋或測試規則。 如果清除這個勾選框，則會在每次套用報告、搜尋或規則測試時剖析內容。
日誌來源	如果有多個日誌來源與此事件相關聯，則此欄位指定術語「多個」，以及日誌來源的數目。
RegEx	您要從有效負載擷取資料時使用的正規表示式。 正規表示式是區分大小寫的。 下列範例顯示樣本正規表示式： • 電子郵件：(.+@[^\.].*\.[a-z]{2,}$) • URL：(http\://[a-zA-Z0-9\-\.]+\.[a-zA-Z]{2,3}(/\S*)?$) • 網域名稱：(http[s]?://(.+?)["/?:]) • 浮點數字：([-+]?\d*\.?\d*$) • 整數：([-+]?\d*$) • IP 位址：(\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b) 擷取群組必須以括弧括住。
擷取群組	擷取群組將多個字元視爲一個單元。 在擷取群組中，於一組括弧內分組字元。

表 49. 「自訂事件內容」視窗參數 (Regex) (繼續)

參數	說明
已啓用	如果清除此勾選框，則此自訂內容不會顯示在搜尋過濾器或直欄清單中，且不會從有效負載剖析內容。

程序

1. 按一下**日誌活動**標籤。
2. 如果您正在串流模式中檢視事件或流程，請按一下**暫停**圖示以暫停串流。
3. 按兩下要作爲自訂內容基準的事件或流程。
4. 按兩下要作爲自訂內容基準的事件。
5. 按一下**擷取內容**。
6. 在**內容類型選擇**窗格中，選取 **Regex 型**選項。
7. 配置自訂內容參數。
8. 按一下**測試**業，以根據有效負載測試正規表示式。
9. 按一下**儲存**。

結果

自訂內容作爲選項顯示於搜尋頁面上的可用直欄清單內。 若要將自訂內容包含在事件或流程清單中，您必須在建立搜尋時，從可用直欄的清單中選取自訂內容。

相關概念:

第 136 頁的『AQL 搜尋字串範例』
使用 Ariel 查詢語言 (AQL) 可從 Ariel 資料庫中的事件、流程和 表格中擷取特定欄位。

建立計算型自訂內容

您可以建立計算型自訂內容，來將有效負載與正規表示式比對。

關於這項作業

在您配置計算型自訂內容時，「自訂事件內容」或「自訂流程內容」視窗會提供下列參數：

表 50. 自訂內容定義視窗參數（計算）

參數	說明
內容定義	
內容名稱	爲此自訂內容鍵入唯一名稱。 新的內容名稱不能是正規化內容的名稱，如使用者名稱、來源 IP 或目的地 IP。
說明	鍵入此自訂內容的說明。
內容計算定義	

表 50. 自訂內容定義視窗參數（計算） (繼續)

參數	說明
內容 1	從清單框中，選取您要在計算中使用的第一個內容。 選項包括所有數值正規化及數值自訂內容。 您也可以指定特定的數值。 從**內容 1** 清單框中，選取**使用者定義**選項。畫面上會顯示**數值內容**參數。鍵入特定的數值。
運算子	從清單框中，選取您要套用至計算中選取的內容的運算子。 選項包括： • 加 • 減 • 乘 • 除
內容 2	從清單框中，選取您要在計算中使用的第二個內容。 選項包括所有數值正規化及數值自訂內容。 您也可以指定特定的數值。 從**內容 1** 清單框中，選取**使用者定義**選項。畫面上會顯示**數值內容**參數。鍵入特定的數值。
已啓用	選取此勾選框可啓用此自訂內容。 如果清除此勾選框，則此自訂內容不會顯示在事件或流程搜尋過濾器或直欄清單中，且不會從有效負載剖析事件或流程內容。

程序

1. 選擇下列其中一項：按一下**日誌活動**標籤。
2. 選用項目。 如果您正在串流模式中檢視事件或流程，請按一下**暫停**圖示以暫停串流。
3. 按兩下要作爲自訂內容基準的事件或流程。
4. 按一下**擷取內容**。
5. 在「內容類型選擇」窗格中，選取**計算型**選項。
6. 配置自訂內容參數。
7. 按一下**測試**，以根據有效負載測試正規表示式。
8. 按一下**儲存**。

結果

自訂內容現在顯示爲搜尋頁面上可用直欄的清單中的選項。 若要將自訂內容包含在事件或流程清單中，您必須在建立搜尋時，從可用直欄的清單中選取自訂內容。

修改自訂內容

您可以修改自訂內容。

關於這項作業

您可以使用「自訂事件內容」或「自訂流程內容」視窗來修改自訂內容。

下表中說明了自訂內容。

表 51. 自訂內容視窗欄

直欄	說明
內容名稱	指定此自訂內容的唯一名稱。
類型	指定此自訂內容的類型。
內容說明	指定此自訂內容的說明。
日誌來源類型	指定此自訂內容適用的日誌來源類型的名稱。 此欄僅顯示在「自訂事件內容」視窗上。
日誌來源	指定此自訂內容適用的日誌來源。 如果有多個日誌來源與此事件或流程相關聯，則此欄位指定術語「多個」，以及日誌來源的數目。 此欄僅顯示在「自訂事件內容」視窗上。
表示式	指定此自訂內容的表示式。 表示式視自訂內容類型而定： 對於 regex 型自訂內容，此參數指定您要從有效負載擷取資料時使用的正規表示式。 對於計算型自訂內容，此參數指定您要建立自訂內容值時使用的計算。
使用者名稱	指定建立此自訂內容的使用者的名稱。
已啓用	指定是否啓用此自訂內容。 此欄位指定爲 True 還是 False。
建立日期	指定建立此自訂內容的日期。
修改日期	指定前次修改此自訂內容的時間。

「自訂事件內容」與「自訂流程內容」工具列提供下列功能：

表 52. 自訂內容工具列選項

選項	說明
加	按一下**新增**以新增自訂內容。
編輯	按一下**編輯**以編輯選取的自訂內容。
副本	按一下**複製**以複製選取的自訂內容。
刪除	按一下**刪除**以刪除選取的自訂內容。

表 52. 自訂內容工具列選項 (繼續)

選項	說明
啓用/停用	按一下**啓用/停用**以啓用或停用在搜尋過濾器或直欄清單中剖析及檢視的所選自訂內容。

程序

1. 選擇下列其中一項：
   - 按一下**日誌活動**標籤。
   - 按一下**網路活動**標籤。
2. 從**搜尋**清單框中，選取**編輯搜尋**。
3. 按一下**管理自訂內容**。
4. 選取要編輯的自訂內容，然後按一下**編輯**。
5. 編輯必要的參數。
6. 選用項目。 如果已編輯正規表示式，請按一下**測試**，以根據有效負載測試正規表示式。
7. 按一下**儲存**。

複製自訂內容

若要建立基於現有自訂內容的新自訂內容，您可以複製現有的自訂內容，然後修改參數。

程序

1. 選擇下列其中一項：
   - 按一下**日誌活動**標籤。
   - 按一下**網路活動**標籤。
2. 從**搜尋**清單框中，選取**編輯搜尋**。
3. 按一下**管理自訂內容**。
4. 選取您要複製的自訂內容，然後按一下**複製**。
5. 編輯必要的參數。
6. 選用項目。 如果您已編輯正規表示式，請按一下**測試**，以根據有效負載測試正規表示式。
7. 按一下**儲存**。

刪除自訂內容

您可以刪除任何自訂內容，前提是此自訂內容與其他自訂內容不關聯。

程序

1. 選擇下列其中一項：
   - 按一下**日誌活動**標籤。
   - 按一下**網路活動**標籤。
2. 按一下**日誌活動**標籤。

3. 從**搜尋**清單框中，選取**編輯搜尋**。
4. 按一下**管理自訂內容**。
5. 選取您要刪除的自訂內容，然後按一下**刪除**。
6. 按一下**是**。

第 11 章 規則管理

從**日誌活動**、**網路活動**及**攻擊**標籤中，您可以檢視及維護規則。

此主題適用於擁有**檢視自訂規則**或**維護自訂規則**使用者角色許可權的使用者。

規則許可權考量

如果具有「檢視自訂規則」及「維護自訂規則」使用者角色許可權，您可以檢視及管理您可存取的網路區域的規則。

若要建立異常偵測規則，您必須對要在其上建立規則的標籤具有適當的**維護自訂規則**許可權。 例如，爲了能夠在「日誌活動」標籤上建立異常偵測規則，您必須具有**日誌活動 > 維護自訂規則**。

如需使用者角色許可權的相關資訊，請參閱 *IBM Security QRadar SIEM Administration Guide*。

規則概觀

規則可對事件、流程或攻擊執行測試，如果測試的所有條件都符合，規則會產生回應。

每個規則中的測試也可以參照其他建置區塊及規則。 您無需以任何特定的順序建立規則，因爲每次新增、編輯或刪除新規則時，系統會檢查相依關係。 如果其他規則參照的規則已刪除或已停用，畫面上會顯示警告，無需執行任何動作。

如需預設規則的完整清單，請參閱 *IBM Security QRadar SIEM Administration Guide*。

規則種類

規則有兩種種類：自訂規則及異常規則。

自訂規則可對事件、流程及攻擊執行測試，以偵測網路中的異常活動。

異常偵測規則可對已儲存流程或事件搜尋的結果執行測試，作爲在網路中發生異常資料流量型樣時進行偵測的方法。

異常偵測規則可對已儲存流程或事件搜尋的結果執行測試，作爲在網路中發生異常資料流量型樣時進行偵測的方法。此規則種類包含下列規則類型：異常、臨界值及行爲。

異常規則會測試異常活動的事件及流程資料流量，例如有新的或不明的資料流量突然停止，或物件處於作用中狀態的時間量百分比變更。例如，您可以建立異常規則，來將前 5 分鐘的平均資料流量與前一小時的平均資料流量比較。 如果變更超過 40%，規則會產生回應。

臨界值規則可測試小於、等於或大於所配置臨界值或位於指定範圍之活動的事件及流程資料流量。臨界值可以基於收集的任何資料。 例如，您可以建立臨界值規則，指定在 8 am 至 5 pm 之間登入伺服器的用戶端不能超過 220 個。 在第 221 個用戶端嘗試登入時，臨界值規則會產生警示。

行爲規則測試一般週期性型樣發生的行爲中流量變更的事件及流程資料流量。例如，如果郵件伺服器通常在午夜每秒與 100 個主機進行通訊，然後突然每秒開始與 1,000 個主機進行通訊，則行爲規則會產生警示。

規則類型

有四種不同的規則類型：事件、流程、共用及攻擊。

事件規則

在事件處理器即時處理事件時，事件規則對事件執行測試。您可以建立事件規則以偵測單一事件（在特定內容中）或事件順序。 例如，如果您要監視網路是否有不成功的登入嘗試，存取多個主機或被不當利用的偵察事件，您可以建立事件規則。 通常是建立攻擊作爲回應的事件規則。

流程規則

在 QFlow Collector 即時處理流程時，流程規則對流程執行測試。 您可以建立流程規則以偵測單一流程（在特定內容中）或流程順序。 通常是建立攻擊作爲回應的流程規則。

共用規則

共用規則對事件與流程記錄的共用欄位執行測試。例如，您可以建立共用規則，以偵測具有特定來源 IP 位址的事件及流程。通常是建立攻擊作爲回應的共用規則。

攻擊規則

只有在對攻擊進行變更時（如，在新事件新增或系統已排定攻擊進行重新評量時），攻擊規則才會處理攻擊。 通常是以電子郵件傳送通知作爲回應的攻擊規則。

規則條件

每個規則可能包含功能、建置區塊或測試。

透過功能，您可以使用建置區塊及其他規則來建立多事件、多流程或多攻擊功能。您可以使用支援布林運算子（如 OR 及 AND）的功能連接規則。 例如，如果要連接事件規則，您可以在事件符合下列規則功能的 anylall 時使用。

建置區塊是沒有回應的規則，用作多個使用者中的共用變數，或建置您要在其他規則中使用的複式規則或邏輯。 您可以將測試群組儲存爲與其他功能搭配使用的建置區塊。建置區塊將讓您重複使用其他規則中的規則測試。 例如，您可以儲存包含網路中所有郵件伺服器 IP 位址的建置區塊，然後使用該建置區塊將這些郵件伺服器從其他規則排除。提供預設建置區塊作爲準則，這應根據網路需要進行檢閱及編輯。

註：依預設，不會載入建置區塊。 定義規則以建置建置區塊。

如需建置區塊的完整清單，請參閱 *IBM Security QRadar SIEM Administration Guide*。

您可以對事件、流程或攻擊的內容（如來源 IP 位址、事件嚴重性或比率分析）執行測試。

規則回應

規則條件符合時，規則可以產生一個以上回應。

規則可以產生下列一個以上回應：

- 建立攻擊。
- 傳送電子郵件。
- 使用「儀表板」功能產生系統通知。
- 將資料新增至參照集。
- 將資料新增至參照資料收集。
- 產生外部系統的回應。
- 將資料新增至可以在規則測試中使用的參照資料收集。
- 執行自訂動作 Script 以回應事件。

參照資料收集類型

您必須先使用指令行介面 (CLI) 建立參照資料收集，然後才能配置將資料傳送至參照資料收集的規則回應。 QRadar 支援下列資料收集類型：

參照集 衍生自網路上發生的事件及流程的元素集，如 IP 位址或使用者名稱清單。

參照對映
資料儲存在將索引鍵對映至值的記錄中。 例如，若要將網路上的使用者活動相關聯，您可以建立參照對映，以使用**使用者名稱**參數作爲索引鍵，使用者的**廣域 ID** 作爲值。

集的參照對映
資料儲存在將索引鍵對映至多個值的記錄中。 例如，若要測試某個專利的授權存取權，請使用自訂事件內容：**專利 ID** 作爲索引鍵，**使用者名稱**參數作爲值。使用集的對映移入授權的使用者清單。

對映的參照對映
資料儲存在將一個索引鍵對映至另一個索引鍵，然後再對映至單一值的記錄中。 例如，若要測試網路頻寬違規，您可以建立對映的對映。 使用**來源 IP** 參數作爲第一個索引鍵，**應用程式**參數作爲第二個索引鍵，**位元組總數**參數作爲值。

參照表格
在參照表格中，資料儲存在將一個索引鍵對映至另一個索引鍵，然後再對映至單一值的表格中。 第二個索引鍵具有指派的類型。 此對映類似於資料庫表格，其中表格中的每個直欄與類型相關聯。 例如，您可以建立參照表格以將**使用者名稱**參數儲存爲第一個索引鍵，且其多個次要索引鍵具有使用者定義的已指派類型，如 **IP 類型**，其中 **來源 IP** 或**來源埠**參數作爲值。 您可以配置新增表格中定義的一個以上索引鍵的規則回應。 您也可以將自訂值新增至規則回應。自訂值必須對次要索引鍵的類型有效。

註：如需參照集及參照資料收集的相關資訊，請參閱您的產品的《*管理手冊*》。

檢視規則

您可以檢視規則的詳細資料，包括測試、建置區塊與回應。

開始之前

視您的使用者角色許可權而定，您可以透過**攻擊**、**日誌活動**或**網路活動**標籤存取規則頁面。

如需使用者角色許可權的相關資訊，請參閱*IBM Security QRadar SIEM Administration Guide*。

關於這項作業

「規則」頁面顯示規則及其關聯的參數清單。若要尋找您要開啓的規則並檢視其詳細資料，則可以使用群組清單框，或工具列上的**搜尋規則**欄位。

程序

1. 選擇下列其中一個選項：
   - 按一下**攻擊**標籤，然後按一下導覽功能表上的**規則**。
   - 按一下**日誌活動**標籤，然後從工具列上的**規則**清單框選取**規則**。
   - 按一下**網路活動**標籤，然後從工具列上的**規則**清單框選取**規則**。
2. 從**顯示**清單框中，選取**規則**。
3. 按兩下您要檢視的規則。
4. 檢查規則的詳細資料。

結果

如果您具有**檢視自訂規則**的許可權，但沒有**維護自訂規則**的許可權，則會顯示**規則摘要**頁面，但無法編輯規則。 如果您有**維護自訂規則**的許可權，則會顯示**規則測試堆疊編輯器**頁面。 您可以檢查和編輯規則的詳細資料。

建立規則

規則會根據規則測試條件來評估送入的資料，以從系統產生回應。符合規則的條件時，可以採取數個動作。例如，您可以配置系統對規則的回應，範圍從產生攻擊、傳送電子郵件、開始掃描、新增參照資料到提高或降低嚴重性之類的值。

開始之前

若要建立新規則，您必須具有**攻擊 > 維護自訂規則**許可權。

關於這項作業

定義規則測試時，請以處理搜尋的相同方式來處理規則，並根據可能的最少資料來進行測試。以這種方式測試可協助規則測試效能並確保不建立昂貴的規則。若要最佳化效能，請從擴大種類開始，從而縮小規則測試所評估的資料範圍。例如，從針對特定日誌來源類型、網路位置、流程來源或環境定義（R2L、L2R、L2L）的規則測試開始。您所做的任何中型測試可能包括 IP 位址、埠資料流量或任何其他相關聯的測試。保留有效負載及正規表示式測試作爲最後一個規則測試。

大部分規則測試可評估單一條件，例如參照資料收集中是否存在元素，或根據事件內容來測試值。對於複雜的比較，您可以透過使用 WHERE 子句條件來建置 Ariel Query Language (AQL) 查詢，以測試事件規則。可使用所有 WHERE 子句函數來撰寫複雜的準則，而不需要執行數個個別測試。例如，使用 AQL WHERE 子句來檢查是否正在參照集上追蹤入埠 SSL 或 Web 資料流量。

程序

1. 從**攻擊**、**日誌活動**或**網路活動**標籤，按一下**規則**。
2. 從**動作**清單中，選取規則類型。

   每一個規則類型都會根據不同來源中送入的資料即時進行測試。例如，事件規則測試送入的日誌來源資料，而攻擊規則測試攻擊的參數以觸發更多回應。
3. 在「規則測試堆疊編輯器」頁面上的「規則」窗格中，在**套用**文字框中輸入您要指派給這個規則的唯一名稱。
4. 從清單框中，選取**區域**或**廣域**。

   區域規則將事件和流程傳送給區域事件處理器以觸發規則。這是預設動作。

   廣域規則將事件及流程傳送給中央事件處理器，這可能會降低主控台上的效能。主控台上的自訂規則引擎 (CRE) 會追蹤部署中每個受管理主機提供的事件相符項。因爲進行部分符合或需要更新計數器，每個受管理主機都會將更新傳送給主控台上的 CRE。當整體規則變成 True 時，主控台會觸發規則回應。

   如需區域和廣域規則測試的相關資訊，請參閱*IBM Security QRadar SIEM Administration Guide*
5. 從**測試群組**清單中，選取您要新增至此規則的一個以上測試。CRE 依序逐行評估規則測試。第一個測試評估爲 True 時，就會評估下一行，直到到達最後一個測試爲止。

   如果您針對新事件規則選取**當事件符合這個 AQL 過濾查詢**測試時，請在**輸入 AQL 過濾查詢**文字框中輸入 AQL WHERE 子句查詢。

   進一步瞭解使用未偵測到之事件的規則：

   可以個別觸發下列規則測試，但是不會遵照同一規則測試堆疊中的後續規則測試。
   - **當一個以上日誌來源類型在這些秒數內未偵測到事件時**
   - **當一個以上日誌來源在這些秒數內未偵測到事件時**
   - **當一個以上日誌來源群組在這些秒數內未偵測到事件時**

   這些規則測試並非由送入的事件啓動，而是在您配置的特定事件間隔內未看到特定事件時啓動。QRadar 使用*監控程式作業*，定期查詢最後一次看到某個事件的時間（最後一次看到的時間），並對每一個日誌來源儲存該事件的這個事件。當這個最後一次看到的時間與現行時間之間的差異超出在規則中配置的秒數時，會觸發該規則。
6. 若要匯出配置的規則作爲建置區塊以與其他規則搭配使用，請按一下**匯出為建置區塊**。

建置區塊是沒有任何回應的規則測試子集。將建置區塊視爲一組可在其他規則中使用的重複使用規則測試。一般範例是在 BB:Host Definition 建置區塊中移入伺服器位址。然後，管理者可以依特定伺服器類型（例如 VPN 伺服器、郵件伺服器或 LDAP 伺服器）來排除或併入規則測試。

7. 在「規則回應」頁面上，配置您希望此規則產生的回應。

   規則回應是所有規則測試都爲 True 時，QRadar 軟體驅動裝置所採取的動作。對於處理器上的區域規則，以及主控台上的廣域規則，當其中的規則變成 Ture 時，會發生電子郵件、syslog 訊息及轉遞事件之類的規則回應。

相關概念:

第 178 頁的『規則回應頁面參數』
爲「規則回應」頁面配置參數，以指定您要 IBM Security QRadar 在某規則被觸發時如何回應。

建立異常偵測規則

使用「異常偵測規則」精靈來建立規則，以透過使用「日期和時間」測試套用時間範圍準則。

開始之前

若要建立新的異常偵測規則，您必須符合下列需求：

- 具有「維護自訂規則」許可權。
- 執行分組搜尋。

在您執行分組搜尋及儲存搜尋準則之後，異常偵測選項會顯示。

關於這項作業

您必須具有適當的角色許可權，才能建立異常偵測規則。

若要在**日誌活動**標籤上建立異常偵測規則，您必須具有**日誌活動維護自訂規則**角色許可權。

若要在**網路活動**標籤上建立異常偵測規則，您必須具有**網路維護自訂規則**角色許可權。

異常偵測規則使用規則所依據的已儲存搜尋準則中的所有分組及過濾器準則，但不使用搜尋準則中的任何時間範圍。

在您建立異常偵測規則時，規則會移入預設測試堆疊。 您可以編輯預設測試，或將測試新增至測試堆疊。 測試堆疊中必須包含至少一項「累計內容」測試。

依預設，「規則測試堆疊編輯器」頁面上已選取**分別測試每個 [群組] 的 [選取的累計內容] 值**。

這會導致異常偵測規則分別測試每個事件或流程群組的所選取累計內容。例如，如果選取的累計值爲 **UniqueCount(sourceIP)**，則規則會測試每個事件或流程群組的每個唯一的來源 IP 位址。

此**分別測試每個 [群組] 的 [選取的累計內容] 值**選項是動態的。 **[選取的累計內容]** 值視您爲預設測試堆疊的**此累計內容測試**欄位選取的選項而定。 **[群組]** 值視在已儲存的搜尋準則中指定的分組選項而定。 如果包含多個分組選項，文字可能會被截斷。 將滑鼠指標移在文字上以檢視所有群組。

程序

1. 按一下**日誌活動** 或**網路活動**標籤。
2. 執行搜尋。
3. 從**規則**功能表中，選取您要建立的規則類型。 選項包括：
   - 新增異常規則
   - 新增臨界值規則
   - 新增行爲規則
4. 閱讀「規則」精靈上的介紹文字。 按**下一步**。 即已選取您先前選擇的規則。
5. 按**下一步**以檢視「規則測試堆疊編輯器」頁面。
6. 在**請在這裡輸入規則名稱**欄位中，鍵入您要指派給此規則的唯一名稱。
7. 若要將測試新增至規則：
   a. 選用項目。 若要過濾「測試群組」清單框中的選項，請在「鍵入內容以進行過濾」欄位中鍵入您要過濾的文字。
   b. 從「測試群組」清單框中，選取您要新增至此規則的測試類型。
   c. 針對您要新增至規則的每個測試，選取測試旁邊的 + 號。
   d. 選用項目。 若要將測試識別爲排除的測試，請在測試開始時在「規則」窗格中按一下 and。 and 會顯示爲 and not。
   e. 按一下畫底線的可配置參數，以自訂測試的變數。
   f. 從對話框中，選取變數的值，然後按一下**提交**。
8. 選用項目。 若要測試每一個事件或流程群組的所選取累計內容總計，請清除**分別測試每個 [群組] 的 [所選取累計內容] 值**勾選框。
9. 在群組窗格中，選取您要爲其指派此規則的群組的勾選框。 如需相關資訊，請參閱規則群組管理。
10. 在**附註**欄位中，鍵入您要爲此規則包含的任何附註。 按**下一步**。
11. 在「規則回應」頁面上，配置您希望此規則產生的回應。 第 178 頁的『規則回應頁面參數』
12. 按**下一步**。
13. 檢閱配置的規則。 按一下**完成**。

規則管理作業

您可以管理自訂及異常規則。

您可以根據需要啓用及停用規則。 您也可以編輯、複製或刪除規則。

您只能在**日誌活動**及**網路活動**標籤上建立異常偵測規則。

若要管理預設及之前建立的異常偵測規則，您必須使用**攻擊**標籤上的「規則」頁面。

啓用及停用規則

在您調整系統時，可以啓用或停用適當的規則，以確保您的系統產生對您的環境有意義的攻擊。

關於這項作業

您必須具有**攻擊** > **維護自訂規則**角色許可權，才能啓用或停用規則。

程序

1. 按一下**攻擊**標籤。
2. 在導覽功能表上，按一下**規則**。
3. 從**規則**頁面上的**顯示**清單框中，選取**規則**。
4. 選取您要啓用或停用的規則。
5. 從**動作**清單框中，選取**啓用/停用**。

編輯規則

您可以編輯規則來變更規則名稱、規則類型、測試或回應。

關於這項作業

您必須具有**攻擊** > **維護自訂規則**角色許可權，才能啓用或停用規則。

程序

1. 按一下**攻擊**標籤。
2. 在導覽功能表上，按一下**規則**。
3. 從**規則**頁面上的**顯示**清單框中，選取**規則**。
4. 按兩下您要編輯的規則。
5. 從**動作**清單框中，選取**開啓**。
6. 選用項目。 如果您要變更規則類型，請按**上一步**，並選取新的規則類型。
7. 在「規則測試堆疊編輯器」頁面上，編輯參數。
8. 按**下一步**。
9. 在「規則回應」頁面上，編輯參數。
10. 按**下一步**。
11. 檢閱編輯的規則。 按一下**完成**。

複製規則

您可以複製現有的規則，輸入規則的新名稱，然後根據需要自訂新規則中的參數。

關於這項作業

您必須具有**攻擊** > **維護自訂規則**角色許可權，才能啓用或停用規則。

程序

1. 按一下**攻擊**標籤。
2. 在導覽功能表上，按一下**規則**。
3. 從**顯示**清單框中，選取**規則**。

4. 選取您要複製的規則。
5. 從**動作**清單框中，選取**複製**。
6. 在複製的規則欄位中的「輸入」名稱中，鍵入新規則的名稱。 按一下**確定**。

刪除規則

您可以從系統刪除規則。

關於這項作業

您必須具有**攻擊** > **維護自訂規則**角色許可權，才能啓用或停用規則。

程序

1. 按一下**攻擊**標籤。
2. 在導覽功能表上，按一下**規則**。
3. 從**顯示**清單框中，選取**規則**。
4. 選取您要刪除的規則。
5. 從**動作**清單框中，選取**刪除**。

規則群組管理

如果您是管理者，您可以建立、編輯及刪除規則群組。 將規則或建置區塊分類爲群組可讓您有效地檢視及追蹤您的規則。

例如，您可以檢視與相符性相關的所有規則。

建立新規則時，您可以將規則指派給現有的群組。 如需使用規則精靈指派群組的相關資訊，請參閱建立自訂規則或建立異常偵測規則。

檢視規則群組

在「規則」頁面上，可以過濾規則或建置區塊，以僅檢視屬於特定群組的規則或建置區塊。

程序

1. 按一下**攻擊**標籤。
2. 在導覽功能表上，按一下**規則**。
3. 從**顯示**清單框中，選取要檢視規則還是建置區塊。
4. 從**過濾**清單框中，選取要檢視的群組種類。

建立群組

「規則」頁面提供預設規則群組，但是，您可以建立新的群組。

程序

1. 按一下**攻擊**標籤。
2. 在導覽功能表上，按一下**規則**。
3. 按一下**群組**。
4. 從導覽樹狀結構中，選取您要在其中建立新群組的群組。

5. 按一下**新建群組**。
6. 輸入下列參數的值：
   - **名稱** - 鍵入要指派給新群組的唯一名稱。 此名稱的長度最多可爲 255 個字元。
   - **說明** - 鍵入要指派給此群組的說明。 此說明的長度最多可爲 255 個字元。
7. 按一下**確定**。
8. 選用項目。 若要變更新群組的位置，請按一下新群組，然後將資料夾拖曳至導覽樹狀結構中的新位置。

將項目指派給群組

您可以將選取的規則或建置區塊指派給群組。

程序

1. 按一下**攻擊**標籤。
2. 在導覽功能表上，按一下**規則**。
3. 選取您要指派給群組的規則或建置區塊。
4. 從**動作**清單框中，選取**指派群組**。
5. 選取您要爲其指派規則或建置區塊的群組。
6. 按一下**指派群組**。
7. 關閉**選擇群組**視窗。

編輯群組

您可以編輯群組，以變更名稱或說明。

程序

1. 按一下**攻擊**標籤。
2. 在導覽功能表上，按一下**規則**。
3. 按一下**群組**。
4. 從導覽樹狀結構中，選取您要編輯的群組。
5. 按一下**編輯**。
6. 更新下列參數的值：
   - **名稱** - 鍵入要指派給新群組的唯一名稱。 此名稱的長度最多可爲 255 個字元。
   - **說明** - 鍵入要指派給此群組的說明。 此說明的長度最多可爲 255 個字元。
7. 按一下**確定**。
8. 選用項目。 若要變更群組的位置，請按一下新群組，然後將資料夾拖曳至導覽樹狀結構中的新位置。

將項目複製到其他群組

您可以將規則或建置區塊從一個群組複製到其他群組。

程序

1. 按一下**攻擊**標籤。
2. 在導覽功能表上，按一下**規則**。
3. 按一下**群組**。

4. 從導覽樹狀結構中，選取您要複製到其他群組的規則或建置區塊。
5. 按一下**複製**。
6. 選取您要將規則或建置區塊複製到其中的群組的勾選框。
7. 按一下**複製**。

從群組中刪除項目

您可以從群組中刪除項目。 在您從群組中刪除項目時，僅會從群組中刪除規則或建置區塊；項目在「規則」頁面上仍然可用。

程序

1. 按一下**攻擊**標籤。
2. 在導覽功能表上，按一下**規則**。
3. 按一下**群組**。
4. 使用導覽樹狀結構，導覽至您要刪除的項目並予以選取。
5. 按一下**移除**。
6. 按一下**確定**。

刪除群組

您可以刪除群組。 在您刪除群組時，該群組的規則或建置區塊仍然在「規則」頁面上。

程序

1. 按一下**攻擊**標籤。
2. 在導覽功能表上，按一下**規則**。
3. 按一下**群組**。
4. 使用導覽樹狀結構，導覽至您要刪除的群組。
5. 按一下**移除**。
6. 按一下**確定**。

編輯建置區塊

您可以編輯符合部署需要的任何預設建置區塊。

關於這項作業

建置區塊是可重複使用的規則測試堆疊，您可以併入爲其他規則中的元件。

例如，您可以編輯 BB:HostDefinition: Mail Servers 建置區塊，以識別部署中的所有郵件伺服器。 然後，您可以配置任何規則，以從規則測試中排除郵件伺服器。

程序

1. 按一下**攻擊**標籤。
2. 在導覽功能表上，按一下**規則**。
3. 從**顯示**清單框中，選取**建置區塊**。
4. 按兩下您要編輯的建置區塊。
5. 根據需要更新建置區塊。

6. 按**下一步**。
7. 透過精靈繼續執行。 如需相關資訊，請參閱建立自訂規則。
8. 按一下**完成**。

規則頁面參數

「規則」頁面上的參數說明。

已部署的規則清單提供了每個規則的下列資訊：

表 53. 規則頁面參數

參數	說明
規則名稱	顯示規則的名稱。
群組	顯示爲其指派此規則的群組。如需群組的相關資訊，請參閱規則群組管理。
規則種類	顯示規則的規則種類。 選項包含「自訂規則」及「異常偵測規則」。
規則類型	顯示規則類型。 規則類型包括： • 事件 • 流程 • 共用 • 攻擊 • 異常 • 臨界值 • 行爲式 如需規則類型的相關資訊，請參閱規則類型。
已啓用	指出是啓用還是停用規則。如需啓用及停用規則的相關資訊，請參閱啓用及停用規則。
回應	顯示規則回應（如果有的話）。 規則回應包括： • 分派新事件 • 電子郵件 • 日誌通知 • SNMP • 參照集 • 參照資料 • IF-MAP 回應 如需規則回應的相關資訊，請參閱規則回應。
事件/流程計數	顯示在規則導致攻擊時，與此規則相關聯的事件或流程數目。
攻擊計數	顯示此規則產生的攻擊數目。
來源	顯示此規則是預設規則（系統）還是自訂規則（使用者）。

表 53. 規則頁面參數 (繼續)

參數	說明
建立日期	指定建立此規則的日期和時間。
修改日期	指定修改此規則的日期和時間。

規則頁面工具列

您可以使用「規則」頁面工具列顯示規則、建置區塊或群組。 您可以管理規則群組及使用規則。

「規則」頁面工具列提供下列功能：

表 54. 規則頁面工具列功能

功能	說明
顯示	從清單框中，選取您要在規則清單中顯示規則還是建置區塊。
群組	從清單框中，選取要在規則清單中顯示的規則群組。
群組	按一下**群組**可管理規則群組。
動作	按一下**動作**，然後選取下列其中一個選項： • **新建事件規則** - 選取此選項可建立新的事件規則。 • **新建流程規則** - 選取此選項可建立新的流程規則。 • **新建共用規則** - 選取此選項可建立新的共用規則。 • **新建攻擊規則** - 選取此選項可建立新的攻擊規則。 • **啓用/停用** - 選取此選項可啓用或停用選取的規則。 • **重複** - 選取此選項可複製選取的規則。 • **編輯** - 選取此選項可編輯選取的規則。 • **刪除** - 選取此選項可刪除選取的規則。 • **指派群組** - 選取此選項可將選取的規則指派給規則群組。
回復規則	按一下**回復規則**可將修改的系統規則回復爲預設值。 在您按一下**回復規則**時，畫面上會顯示確認視窗。 在您回復規則時，之前的任何修改會永久移除。 若要回復規則及維護修改的版本，請複製規則，並使用已修改規則上的**回復規則**選項。

表 54. 規則頁面工具列功能 (繼續)

功能	說明
搜尋規則	在**搜尋準則**欄位中鍵入搜尋準則，然後按一下**搜尋準則**圖示或按鍵盤上的 Enter。 與搜尋準則相符的所有規則都會顯示在規則清單中。 搜尋下列參數，以取得符合您的搜尋準則的項目： • 規則名稱 • 規則（說明） • 附註 • 回應 「搜尋規則」功能會嘗試尋找直接字串相符項。 如果找不到相符項，則「搜尋規則」功能會嘗試正規表示式 (Regex) 相符項。

規則回應頁面參數

爲「規則回應」頁面配置參數，以指定您要 IBM Security QRadar 在某規則被觸發時如何回應。

註：當您建置 AQL 查詢時，如果您從任何文件中複製包含單引號的文字，並將文字貼上至 IBM Security QRadar，則您的查詢將不會進行剖析。您可以使用暫行解決方法，將文字貼上至 QRadar，並重新輸入單引號，或者可以從 IBM Knowledge Center 複製並貼上文字。

下表提供「規則回應」頁面參數。

表 55. 「事件」、「流程」及「共用規則回應」頁面參數

參數	說明
標註事件	如果您要將註釋新增至此事件，請選取此勾選框，然後鍵入要新增至事件的註釋。
捨棄偵測到的事件	選取此勾選框可將事件（通常傳送至 Magistrate 元件）強制傳送至 Ariel 資料庫以進行報告或搜尋。捨棄的事件會寫入儲存體並略過規則測試。 此事件不會顯示在**攻擊**標籤上。
分派新事件	選取此勾選框可分派新的事件以及原始事件或流程，處理方式如同系統中的所有其他事件。 選取此勾選框可分派新的事件以及原始事件，處理方式如同系統中的所有其他事件。 在您選取此勾選框時，畫面上會顯示**分派新事件**參數。 依預設，勾選框會清除。
事件名稱	鍵入您要在**攻擊**標籤上顯示的事件的唯一名稱。

表 55. 「事件」、「流程」及「共用規則回應」頁面參數 (繼續)

參數	說明
事件說明	鍵入事件的說明。 說明會顯示在事件詳細資料的「註釋」窗格中。
嚴重性	從清單框中，選取事件的嚴重性。 範圍爲 0（最低）至 10（最高），預設值爲 0。「嚴重性」顯示在事件詳細資料的「註釋」窗格中。
可靠性	從清單框中，選取事件的可靠性。 範圍爲 0（最低）至 10（最高），預設值爲 10。 可靠性會顯示在事件詳細資料的「註釋」窗格中。
關聯	從清單框中，選取事件的相關性。 範圍爲 0（最低）至 10（最高），預設值爲 10。 相關性會顯示在事件詳細資料的「註釋」窗格中。
高階種類	從清單框中，選取您希望此規則在處理事件時使用的高階事件種類。
低階種類	從清單框中，選取您希望此規則在處理事件時使用的低階事件種類。
標註此攻擊	選取此勾選框可將註釋新增至此攻擊，然後鍵入註釋。
電子郵件	選取此勾選框可顯示電子郵件選項。 **註**：若要變更**電子郵件語言環境**設定，請在**管理**標籤上選取**系統設定**。
輸入要通知的電子郵件位址	鍵入電子郵件位址，以在此規則產生時傳送通知。 請使用逗點區隔多個電子郵件位址。
選取事件/流程電子郵件範本	選取與此規則相關聯的電子郵件之電子郵件範本。如需配置自訂電子郵件通知的相關資訊，請參閱 *IBM Security QRadar SIEM Administration Guide*。
SNMP 設陷	只有在系統設定中配置「SNMP 設定」參數時，才顯示此參數。 選取此勾選框可啓用此規則，來傳送 SNMP 通知（設陷）。 SNMP 設陷輸出包括系統時間、設陷 OID 及通知資料（如 MIB 所定義）。
傳送至本端 SysLog	如果您要在本端記載事件或流程，請選取此勾選框。 依預設，此勾選框會清除。 **註**：只能在軟體驅動裝置上本端記載正規化事件。 如果要傳送未處理的事件資料，您必須使用「傳送至轉遞目的地」選項以將資料傳送至遠端 syslog 主機。
傳送至轉遞目的地	如果您要在轉遞目的地上記載事件或流程，請選取此勾選框。轉遞目的地是供應商系統，如 SIEM、通行證或警示系統。在您選取此勾選框時，畫面上會顯示轉遞目的地清單。 請選取您要傳送此事件或流程至其中的轉遞目的地的勾選框。 若要新增、編輯或刪除轉遞目的地，請按一下**管理目的地**鏈結。

表 55. 「事件」、「流程」及「共用規則回應」頁面參數 (繼續)

參數	說明
通知	如果您希望產生的事件（作爲此規則的結果）顯示在「儀表板」標籤上的「系統通知」項目中，請選取此勾選框。 如果您啓用通知，請配置**回應限制器**參數。
新增至參照集	如果您希望產生的事件（作爲此規則的結果）將資料新增至參照集，請選取此勾選框。 若要將資料新增至參照集： 1. 使用第一個清單框，選取您要新增的資料。選項包括所有正規化或自訂資料。 2. 使用第二個清單框，選取設定爲您要新增指定的資料至其中的參照。 **新增至參照集**規則回應提供下列功能： **重新整理** 按一下**重新整理**可重新整理第一個清單框，來確保此清單是最新的。 **配置參照集** 按一下**配置參照集**可配置參照集。 只有在您具有管理許可權時，此選項才可用。
新增至參照資料	您必須先使用指令行介面 (CLI) 建立參照資料收集，然後才能使用此規則回應。 如需如何建立及使用參照資料收集的相關資訊，請參閱您的產品的《*管理手冊*》。 如果您希望產生的事件（作爲此規則的結果）新增至參照資料收集，請選取此勾選框。 在您選取勾選框之後，選取下列其中一個選項： **新增至參照對映** 選取此選項可將資料傳送至單一索引鍵/多個值配對的集合。 您必須選取資料記錄的索引鍵及值，然後選取要將資料記錄新增至其中的參照對映。 **新增至集合的參照對映** 選取此選項可將資料傳送至索引鍵/單一值配對的集合。 您必須選取資料記錄的索引鍵及值，然後選取要將資料記錄新增至其中的集的參照對映。 **新增至對映的參照對映** 選取此選項可將資料傳送至多個索引鍵/單一值配對的集合。 您必須選取第一個對映的索引鍵、第二個對映的索引鍵及資料記錄的值。 您還必須選取要將資料記錄新增至其中的對映的參照對映。 **新增至參照表格** 選取此選項可將資料傳送至多個索引鍵/單一值配對的集合，其中類型已指派給次要索引鍵。 選取您要將資料新增至其中的參照表格，然後選取主要索引鍵。 選取資料記錄的內部索引鍵（次要索引鍵）及其值。

表 55. 「事件」、「流程」及「共用規則回應」頁面參數 (繼續)

參數	說明
執行自訂動作	您可以撰寫 Script 以執行特定動作來回應網路事件。例如，您可以撰寫 Script 來建立防火牆規則，以封鎖您網路中的特定來源 IP 位址以回應重複的登入失敗。 選取此勾選框，然後從**要執行的自訂動作**清單中選取自訂動作。 您可以使用**管理**標籤上的**定義動作**圖示來新增及配置自訂動作。
在 IF-MAP 伺服器上發佈	如果在系統設定中配置及部署 IF-MAP 參數，請選取此選項來發佈有關 IF-MAP 伺服器的事件資訊。
回應限制器	選取此勾選框，然後使用清單框來配置您希望此規則回應的頻率。
啓用規則	選取此勾選框可啓用此規則。

如果規則類型爲「攻擊」，下表提供了「規則回應」頁面參數。

表 56. 攻擊規則回應頁面參數

參數	說明
命名/標註偵測到的攻擊	選取此勾選框可顯示「命名」選項。
新建攻擊名稱	鍵入您要指派給攻擊的名稱。
攻擊註釋	鍵入您要在「攻擊」標籤上顯示的攻擊註釋。
攻擊名稱	選取下列其中一個選項： **此資訊應提出攻擊的名稱** 如果您希望「事件名稱」資訊提出攻擊名稱，請選取此選項。 **此資訊應設定或取代攻擊的名稱** 如果您希望配置的「事件名稱」成爲攻擊名稱，請選取此選項。
電子郵件	選取此勾選框可顯示電子郵件選項。 **註**：若要變更**電子郵件語言環境**設定，請在**管理**標籤上選取**系統設定**。
輸入要通知的電子郵件位址	鍵入電子郵件位址，以在事件產生時傳送通知。 請使用逗點區隔多個電子郵件位址。
SNMP 設陷	只有在系統設定中配置「SNMP 設定」參數時，才顯示此參數。 選取此勾選框可啓用此規則，來傳送 SNMP 通知（設陷）。對於攻擊規則，SNMP 設陷輸出包括系統時間、設陷 OID 及通知資料（如 MIB 所定義）。
傳送至本端 SysLog	如果您要在本端記載事件或流程，請選取此勾選框。

表 56. 攻擊規則回應頁面參數 (繼續)

參數	說明
傳送至轉遞目的地	如果您要在轉遞目的地上記載事件或流程，請選取此勾選框。轉遞目的地是供應商系統，如 SIEM、通行證或警示系統。在您選取此勾選框時，畫面上會顯示轉遞目的地清單。 請選取您要傳送此事件或流程至其中的轉遞目的地的勾選框。 若要新增、編輯或刪除轉遞目的地，請按一下**管理目的地**鏈結。
在 IF-MAP 伺服器上發佈	如果在系統設定中配置及部署 IF-MAP 參數，請選取此選項來發佈有關 IF-MAP 伺服器的攻擊資訊。
回應限制器	選取此勾選框，然後使用清單框來配置您希望此規則回應的頻率。
啓用規則	選取此勾選框可啓用此規則。 依預設，勾選框已選取。

如果規則類型爲「異常」，下表提供了「規則回應」頁面參數。

表 57. 異常偵測規則回應頁面參數

參數	說明
分派新事件	指定此規則分派新的事件以及原始事件或流程，處理方式如同系統中的所有其他事件。依預設，此勾選框已選取，且無法清除。
事件名稱	鍵入您要在「攻擊」標籤上顯示的事件的唯一名稱。
事件說明	鍵入事件的說明。 說明會顯示在事件詳細資料的「註釋」窗格中。
攻擊命名	選取下列其中一個選項： **此資訊應提出相關聯攻擊的名稱** 如果您希望「事件名稱」資訊提出攻擊名稱，請選取此選項。 **此資訊應設定或取代相關聯攻擊的名稱** 如果您希望配置的「事件名稱」成爲攻擊名稱，請選取此選項。 **註**：取代攻擊的名稱之後，名稱不會變更，除非關閉攻擊。例如，如果攻擊與多個規則相關聯，則最新的事件不會觸發配置爲置換攻擊名稱的規則，並且最後一個事件不會更新攻擊的名稱。攻擊名稱會保留置換規則設定的名稱。 **此資訊不應提出相關聯攻擊的命名** 如果您不希望「事件名稱」資訊提出攻擊名稱，請選取此選項。
嚴重性	範圍爲 0（最低）至 10（最高），預設值爲 5。「嚴重性」顯示在事件詳細資料的「註釋」窗格中。
可靠性	使用清單框選取事件的可靠性。 範圍爲 0（最低）至 10（最高），預設值爲 5。「可靠性」顯示在事件詳細資料的「註釋」窗格中。

表 57. 異常偵測規則回應頁面參數 (繼續)

參數	說明
相關性	使用清單框選取事件的相關性。 範圍爲 0（最低）至 10（最高），預設值爲 5。「相關性」顯示在事件詳細資料的「註釋」窗格中。
高階種類	從清單框中，選取您希望此規則在處理事件時使用的高階事件種類。
低階種類	從清單框中，選取您希望此規則在處理事件時使用的低階事件種類。
標註此攻擊	選取此勾選框可將註釋新增至此攻擊，然後鍵入註釋。
確保分派的事件是攻擊的一部分	作爲此規則的結果，事件會轉遞至 Magistrate 元件。 如果存在攻擊，則會新增此事件。如果「攻擊」標籤上未建立任何攻擊，會建立新的攻擊。 畫面上會顯示下列選項： **索引攻擊基於** 指定新的攻擊基於事件名稱。 依預設，此參數已啓用。 **包含從此刻起 秒內在攻擊中「事件名稱」偵測到的事件** 選取此勾選框，然後鍵入您要在**攻擊**標籤上包含來源中偵測到的事件或流程的秒數。
電子郵件	選取此勾選框可顯示電子郵件選項。 **註**：若要變更**電子郵件語言環境**設定，請在**管理**標籤上選取**系統設定**。
輸入要通知的電子郵件位址	鍵入電子郵件位址，以在此規則產生時傳送通知。 請使用逗點區隔多個電子郵件位址。
選取事件電子郵件範本	選取與此規則相關聯的電子郵件之電子郵件範本。如需配置自訂電子郵件通知的相關資訊，請參閱 *IBM Security QRadar Administration Guide*。
通知	如果您希望產生的事件（作爲此規則的結果）顯示在**儀表板**標籤上的「系統通知」項目中，請選取此勾選框。 如果您啓用通知，請配置**回應限制器**參數。
傳送至本端 SysLog	如果您要在本端記載事件或流程，請選取此勾選框。依預設，勾選框會清除。 **註**：只能在 QRadar 軟體驅動裝置上本端記載正規化事件。如果要傳送未處理的事件資料，您必須使用「傳送至轉遞目的地」選項以將資料傳送至遠端 syslog 主機。

表 57. 異常偵測規則回應頁面參數 (繼續)

參數	說明
新增至參照集	如果您希望產生的事件（作爲此規則的結果）將資料新增至參照集，請選取此勾選框。 若要將資料新增至參照集： 1. 使用第一個清單框，選取您要新增的資料。選項包括所有正規化或自訂資料。 2. 使用第二個清單框，選取設定爲您要新增指定的資料至其中的參照。 **新增至參照集**規則回應提供下列功能： **重新整理** 按一下**重新整理**可重新整理第一個清單框，來確保此清單是最新的。 **配置參照集** 按一下**配置參照集**可配置參照集。 只有在您具有管理許可權時，此選項才可用。
新增至參照資料	您必須先使用指令行介面 (CLI) 建立參照資料收集，然後才能使用此規則回應。 如需如何建立及使用參照資料收集的相關資訊，請參閱您的產品的《*管理手冊*》。 如果您希望產生的事件（作爲此規則的結果）新增至參照資料收集，請選取此勾選框。 在您選取勾選框之後，選取下列其中一個選項： **新增至參照對映** 選取此選項可將資料傳送至單一索引鍵/多個值配對的集合。 您必須選取資料記錄的索引鍵及值，然後選取要將資料記錄新增至其中的參照對映。 **新增至集合的參照對映** 選取此選項可將資料傳送至索引鍵/單一值配對的集合。 您必須選取資料記錄的索引鍵及值，然後選取要將資料記錄新增至其中的集的參照對映。 **新增至對映的參照對映** 選取此選項可將資料傳送至多個索引鍵/單一值配對的集合。 您必須選取第一個對映的索引鍵、第二個對映的索引鍵及資料記錄的值。 您還必須選取要將資料記錄新增至其中的對映的參照對映。 **新增至參照表格** 選取此選項可將資料傳送至多個索引鍵/單一值配對的集合，其中類型已指派給次要索引鍵。 選取您要將資料新增至其中的參照表格，然後選取主要索引鍵。 選取資料記錄的內部索引鍵（次要索引鍵）及其值。

表 57. 異常偵測規則回應頁面參數 (繼續)

參數	說明
執行自訂動作	您可以撰寫 Script 以執行特定動作來回應網路事件。例如，您可以撰寫 Script 來建立防火牆規則，以封鎖您網路中的特定來源 IP 位址以回應重複的登入失敗。 選取此勾選框，然後從**要執行的自訂動作**清單中選取自訂動作。 您可以使用**管理**標籤上的**定義動作**圖示來新增及配置自訂動作。
在 IF-MAP 伺服器上發佈	如果在系統設定中配置及部署 IF-MAP 參數，請選取此選項來發佈有關 IF-MAP 伺服器的攻擊資訊。
回應限制器	選取此勾選框，然後使用清單框來配置您希望此規則回應的頻率
啓用規則	選取此勾選框可啓用此規則。 依預設，勾選框已選取。

SNMP 通知可能類似下列內容：

```
"Wed Sep 28 12:20:57 GMT 2005, Custom Rule Engine Notification -
 Rule 'SNMPTRAPTst' Fired. 172.16.20.98:0 -> 172.16.60.75:0 1, Event Name:
 ICMP Destination Unreachable Communication with Destination Host is
 Administratively Prohibited, QID: 1000156, Category: 1014, Notes:
 Offense description"
```

syslog 輸出可能類似下列內容：

```
Sep 28 12:39:01 localhost.localdomain ECS:
 Rule 'Name of Rule' Fired: 172.16.60.219:12642
 -> 172.16.210.126:6666 6, Event Name: SCAN SYN FIN, QID:
 1000398, Category: 1011, Notes: Event description
```

相關工作:

第 168 頁的『建立規則』

規則會根據規則測試條件來評估送入的資料，以從系統產生回應。符合規則的條件時，可以採取數個動作。例如，您可以配置系統對規則的回應，範圍從產生攻擊、傳送電子郵件、開始掃描、新增參照資料到提高或降低嚴重性之類的值。

第 12 章 歷程關聯

使用歷程關聯來透過自訂規則引擎 (CRE) 執行過去的事件和流程，以識別已發生的威脅或安全事件。

限制： 您無法在 IBM Security QRadar Log Manager 中使用歷程關聯。如需 IBM Security QRadar SIEM 與 IBM Security QRadar Log Manager 之間差異的相關資訊，請參閱第 5 頁的『安全智慧產品中的功能』。

依預設，IBM Security QRadar SIEM 部署會幾近即時地分析從日誌來源和流程來源收集的資訊。您可以使用歷程關聯，透過開始時間或裝置時間來產生關聯。*開始時間*是 QRadar 接收事件的時間。 *裝置時間*是在裝置上發生事件的時間。

歷程關聯在下列狀況中很有用：

分析大量資料

如果要將大量資料載入 QRadar 部署，則可以使用歷程關聯來關聯該資料與即時收集的資料。例如，若要避免正常工作時間內的效能降低，可以在每晚午夜從多個日誌來源載入事件。您可以使用歷程關聯並依裝置時間關聯資料，以查看過去 24 小時內發生的網路事件順序。

測試新規則

您可以執行歷程關聯來測試新規則。例如，您的某一部伺服器最近遭受到新惡意軟體的攻擊，而您尚未對該惡意軟體建立規則。您可以針對該惡意軟體建立測試規則。然後，可以使用歷程關聯來根據歷程資料檢查規則，以查看在攻擊時，該規則是否能觸發回應。類似地，您可以使用歷程關聯來判定第一次攻擊何時發生，或是攻擊的頻率。您可以繼續調整規則，然後將其移至正式作業環境。

重建已遺失或已清除的攻擊

如果您的系統因斷電或其他原因遺失了攻擊，那麼您可以透過對該期間進入的事件和流程執行歷程關聯來重建攻擊。

識別之前隱藏的威脅

瞭解最新安全威脅的相關資訊之後，您可以使用歷程關聯來識別已發生但未觸發事件的網路事件。您可以快速測試以找出已危及您組織系統或資料的威脅。

歷程關聯概觀

可配置歷程關聯設定檔來指定您要分析的歷程資料，以及您要據以測試的規則集。觸發規則時，會建立攻擊。您可以指派攻擊進行調查和補救。

資料選取

設定檔使用已儲存的搜尋來收集歷程事件和流程資料以用於執行。請確保您的安全設定檔授權檢視您要併入歷程關聯執行中的事件和流程。

規則選取與處理

QRadar 主控台只會根據歷程關聯設定檔中指定的規則來處理資料。

事件及流程兩者中的共用規則測試資料。您必須擁有檢視事件及流程兩者的權限，然後才能將共用規則新增至設定檔。當沒有權限檢視事件及流程兩者的使用者編輯設定檔時，系統會自動從設定檔中移除共用規則。

您可以在歷程關聯設定檔中包含停用的規則。當設定檔執行時，會針對送入的事件和流程評估停用的規則。如果規則已觸發，而規則動作是要產生攻擊，則停用了規則也會建立攻擊。若要避免產生不必要的干擾，歷程關聯期間將會忽略規則回應，例如：報告產生和郵件通知。

由於歷程關聯處理在單一位置中進行，因此設定檔中所包含的規則會被視爲廣域規則。該處理不會將規則從區域變更爲廣域，但是在歷程關聯執行期間會將它視同廣域來處理。 部分規則（如有狀態規則）觸發的回應，可能不同於它們在區域事件處理器上執行的正常關聯中觸發的回應。例如，對同一個使用者名稱在 5 分鐘內五次登入失敗進行追蹤的區域有狀態規則，在正常與歷程關聯執行下的行爲會不同。在正常關聯下，此區域規則會保持使用一個計數器，來計算每一個區域事件處理器所接收到的失敗登入數。在歷程關聯中，此規則會針對整個 QRadar 系統保持使用單一計數器。在此狀況下，可能會以不同的方式（相較於正常關聯執行）建立攻擊。

攻擊建立

歷程關聯執行只有在規則被觸發以及規則動作指定必須建立攻擊時才會建立攻擊。即便使用的是相同設定檔，歷程關聯執行也不會造成即時攻擊，亦不會造成因舊版歷程關聯執行而建立的攻擊。

歷程關聯執行可以建立的攻擊數目上限爲 100。歷程關聯執行會在達到此限制時停止。

您可以在「威脅與安全監視」儀表板上檢視歷程攻擊，同時在**攻擊**標籤上檢閱即時攻擊。

建立歷程關聯設定檔

您可以建立歷程關聯設定檔來透過自訂規則引擎 (CRE) 重新執行過去的事件和流程。此設定檔包含在執行期間要使用的資料集及規則的相關資訊。

限制： 您只能在 IBM Security QRadar SIEM 中建立歷程設定檔。您無法在 IBM Security QRadar Log Manager 中建立歷程設定檔。

開始之前

事件及流程兩者中的共用規則測試資料。您必須擁有檢視事件及流程兩者的權限，然後才能將共用規則新增至設定檔。當沒有權限檢視事件及流程兩者的使用者編輯設定檔時，系統會自動從設定檔中移除共用規則。

關於這項作業

您可以將設定檔配置爲透過開始時間或裝置時間來產生關聯。*開始時間*是當事件抵達事件收集器時的時間。*裝置時間*是在裝置上發生事件的時間。可以透過開始時間或裝置時間關聯事件。 只能透過開始時間關聯流程。

您可以在設定檔中包含停用的規則。已停用的規則是以規則清單中的規則名稱後面的（**已停用**）表示。

即便使用的是相同設定檔，歷程關聯執行也不會造成即時攻擊，亦不會造成因舊版歷程關聯執行而建立的攻擊。

程序

1. 開啓「歷程關聯」對話框。
   - 在**日誌活動**標籤上，按一下**動作 > 歷程關聯**。
   - 在**網路活動**標籤上，按一下**動作 > 歷程關聯**。
   - 在**攻擊**標籤上，按一下**規則 > 動作 > 歷程關聯**。
2. 按一下**新增**，然後選取**事件設定檔**或**流程設定檔**。
3. 鍵入設定檔的名稱，然後選取已儲存搜尋。 您只能使用非聚集的已儲存搜尋。
4. 在**規則**標籤上，選取要針對歷程資料執行的規則，然後選擇關聯時間。

   如果您選取**使用所有已啓用規則**勾選框，則無法在設定檔中包含已停用的規則。如果您要在設定檔中包含已啓用及已停用的規則，則必須從規則清單中個別選取它們，然後按一下**新增選取的規則**。
5. 在**排程**標籤上，輸入已儲存搜尋的時間範圍，並設定設定檔排程設定。
6. 在**摘要**標籤上，檢閱配置，並選擇是否立即執行設定檔。
7. 按一下**儲存**。

   設定檔將放置於待處理的佇列中。 根據排程排入佇列的設定檔較手動執行優先進行。

檢視歷程關聯執行的相關資訊

檢視歷程關聯設定檔的歷程來查看設定檔過去的執行的相關資訊。您可以查看在執行期間建立的攻擊清單，以及符合設定檔中所觸發規則之事件或流程的型錄。您可以檢視已排入佇列、執行中、已完成、已完成但有錯誤及已取消之歷程關聯執行的歷程。

關於這項作業

系統會爲在執行期間針對每一個唯一來源 IP 位址所觸發的每一個規則，各建立一個歷程關聯型錄（即使未建立攻擊）。該型錄包含完全或部分符合已觸發規則的所有事件或流程。

您無法從 QRadar 直接建置歷程關聯資料的報告。如果要使用第三方程式來建置報告，可以從 QRadar 匯出資料。

程序

1. 開啓「歷程關聯」對話框。
   - 在**日誌活動**標籤上，按一下**動作 > 歷程關聯**。
   - 在**網路活動**標籤上，按一下**動作 > 歷程關聯**。
   - 在**攻擊**標籤上，按一下**規則 > 動作 > 歷程關聯**。
2. 選取設定檔，然後按一下**檢視歷程**。
   a. 如果歷程關聯執行狀態爲**已完成**，且**攻擊計數**爲 0，則設定檔規則並未觸發任何攻擊。
   b. 如果歷程關聯執行建立了攻擊，請在**攻擊計數**欄中，按一下鏈結以查看已建立的攻擊清單。 如果僅建立一個攻擊，則會顯示攻擊摘要。

3. 在**型錄**欄中，按一下鏈結以查看完全或部分符合設定檔規則的事件清單。

   事件清單中的**開始時間**欄代表 QRadar 接收事件的時間。

4. 按一下**關閉**。

第 13 章 X-Force Threat Intelligence 資訊來源整合

IBM Security X-Force Threat Intelligence 資訊來源提供潛在惡意 IP 位址和 URL 的最新清單。此資訊可合併到規則、攻擊與事件中，用來識別網路環境中的任何非預期活動，以防止它威脅網路的穩定性。

您必須擁有 QRadar 授權才能將 X-Force Threat Intelligence 資訊來源與 QRadar 搭配使用。

X-Force Threat Intelligence 資訊來源中的內容會獲得一個威脅評分，供您用來協助設定透過此內容產生之事件和攻擊的優先順序。來自這些智慧來源的資料自動合併到 QRadar 關聯和分析功能中，並通過網際網路威脅資料增強其威脅偵測功能。涉及這些位址的任何安全事件或網路活動資料將會自動標示，因此將寶貴的環境定義新增至安全事件分析和調查

若要設定威脅的優先順序並識別需要更多檢查的安全事件，您可以選擇將 X-Force 資訊來源合併到 QRadar 規則、攻擊和事件中。 例如，您可以使用資訊來源來識別下列類型的事件：

- 動態範圍 IP 位址的一連串嘗試登入
- 與業務合作夥伴入口網站的匿名 Proxy 連線
- 內部端點與已知 botnet 指令和控制項之間的連線
- 端點與已知惡意軟體發行套件網站之間的通訊

X-Force Threat Intelligence 資訊來源可對 IP 位址進行分類，然後將信任等級值指派給這個分類。將信任係數值 0 - 100 指派給 IP 信譽資料的分類。這個信任值代表 X-Force 對這個 IP 位址中的資料進行精確分類的信任程度。以信任係數值 0 對垃圾郵件進行 IP 信譽分類，表示來源 IP 資料流量絕對不是垃圾郵件，而值爲 100 則表示絕對是垃圾郵件來源。調整規則時，您可以使用信任係數值來調整規則觸發程式的靈敏度。透過調整這個信任係數值來調整產生的攻擊數。

IP 位址分組爲下列種類：

- 惡意軟體主機
- 垃圾郵件來源
- 動態 IP 位址
- 匿名 Proxy
- Botnet 指令和控制項
- 掃描 IP 位址

X-Force Threat Intelligence 資訊來源還對 URL 位址進行分類。 例如，URL 位址可能分類成約會、賭博或色情網站。 若要查看 URL 分類的種類的完整清單，請參閱 IBM X-Force Exchange 網站 (https://exchange.xforce.ibmcloud.com/faq)。

在可以使用 URL 型規則之前，您必須建立自訂事件內容來從有效負載擷取 URL。 已針對來自許多來源（例如 Blue Coat SG 和 Juniper Networks Secure Access）的事件定義 URL 自訂內容。

如需建立自訂事件內容的相關資訊，請參閱自訂事件和流程內容。

X-Force Threat Intelligence 更新項目和伺服器

將 IBM Security X-Force Threat Intelligence 資訊來源新增至 QRadar 之後，您可以立即接收到進階威脅資料。

整體而言，X-Force 中的資料集每 3 分鐘更新一次，而 QRadar 主控台 負責處理所有的外部通訊。

可連接下列伺服器來處理 X-Force 資料更新、授權、儀表板小組件資訊來源及 QRadar 自動更新：

表 58. X-Force 伺服器

連接的伺服器	伺服器說明
www.iss.net	QRadar（AlertCon/RSS 資訊來源）的 X-Force Threat Intelligence 儀表板小組件
update.xforce-security.com	適用於 IP 信譽和 URL 資料的 X-Force Threat Intelligence 資訊來源更新伺服器
license.xforce-security.com	X-Force Threat Intelligence 授權伺服器
qmmunity.q1labs.com	QRadar 自動更新。如需自動更新伺服器的相關資訊，請參閱 www.ibm.com/support (http://www-01.ibm.com/support/docview.wss?uid=swg21958881)。

在 IBM Security QRadar 中啓用 X-Force 規則

可將 X-Force IP 信譽智慧資訊來源授權新增至 QRadar 系統，來新增加強型 X-Force 規則。

程序

1. 按一下**日誌活動**標籤。
2. 在工具列上，按一下**規則 > 規則**。
3. 從**群組**功能表中，按一下 **XForce Premium**。

   群組直欄可能同時顯示舊式和加強規則。依預設，會停用 X-Force 舊式規則。但是，您可能會看到已啓用舊式規則。使用更新的加強規則，而不是利用遠端網路的舊式規則。將移除遠端網路選項。
4. 透過選取規則列並按一下**動作 > 啓用/停用**，來停用任何舊式規則、X-Force Premium 規則。

加強型 X-Force Threat Intelligence 規則

將 X-Force Threat Intelligence 資訊來源新增至 QRadar 之後，您可以開始使用加強 X-Force 規則群組中的規則。

下列規則是**加強型 X-Force 規則**群組的一部分。 它們可以依現狀使用，也可以進行自訂。

下列規則是 IP 型規則：

X-Force Premium：與可能惡意軟體主機的內部連線
此通訊指示嘗試感染用戶端系統或下載惡意軟體的可能性很高。

X-Force Premium：內部主機與匿名 Proxy 通訊
匿名 Proxy 是已知掩蓋身分的位址。 惡意軟體或進階持續性威脅期間通常使用它們來隱藏與外部來源通訊的發起人。 這些位址可能與惡意軟體通訊或資料洩漏等活動相關。

X-Force Premium：內部郵件伺服器傳送郵件到可能的垃圾郵件主機
一般而言，與垃圾郵件主機通訊的郵件伺服器是誤用。

X-Force Premium：非郵件伺服器與已知傳送垃圾郵件的主機通訊
此行爲指示伺服器已受損並被使用作爲垃圾郵件中繼的可能性很高。

X-Force Premium：非伺服器與外部動態 IP 通訊
動態指派的 IP 位址一般與網際網路上的合法伺服器不相關。 與動態位址通訊的內部工作站可能指示可疑的內部或東，或者惡意軟體或僵屍網路活動。

X-Force Premium：伺服器起始的與動態主機的連線
一般而言，伺服器與具有固定身分且不是具有動態 IP 位址的主機通訊。

因爲 URL 是所要傳輸資料的更具體的指示器，所以 URL 型規則比 IP 型規則更精確。

下列規則是 URL 型規則：

X-Force Premium：內部主機與 Botnet 指令和控制項 URL 通訊
合法的伺服器有時可能用來在特定 URL 位址提供僵屍網路連線。

X-Force Premium：內部主機與惡意軟體 URL 通訊
合法的伺服器有時可用來在特定 URL 位址提供惡意軟體。

使用 URL 分類建立規則以監視對特定類型網站的存取

您可以建立一個規則，用於當內部網路中的使用者存取分類爲賭博網站的 URL 位址時傳送電子郵件通知。

開始之前

若要使用 URL 分類規則，您必須訂閱 X-Force Threat Intelligence 資訊來源。

若要建立新規則，您必須具有**攻擊 > 維護自訂規則**許可權。

程序

1. 按一下**攻擊**標籤。
2. 在導覽功能表上，按一下**規則**。
3. 從**動作**清單中，選取**新建事件規則**。
4. 閱讀「規則」精靈上的介紹文字，然後按**下一步**。
5. 按一下**事件**，然後按**下一步**。
6. 從**測試群組**清單框中，選取 **X-Force 測試**。
7. 按一下**當 X-Force 將此 URL 內容分類為下列其中一個種類時**測試旁邊的加號 (+)。
8. 在「規則」窗格的**請在這裡輸入規則名稱**欄位中，鍵入您要指派給此規則的唯一名稱。

9. 從清單框中，選取**本端**或**廣域**。
10. 按一下畫底線的可配置參數，以自訂測試的變數。
    a. 按一下 **URL（自訂）**。
    b. 選取包含從有效負載擷取之 URL 的 URL 內容，然後按一下**提交**。
    c. 按一下**下列其中一個種類**。
    d. 從 X-Force URL 種類中選取**賭博/彩票**，然後按一下 **新增 +**，再按一下**提交**。
11. 若要將配置的規則匯出爲建置區塊，以與其他規則搭配使用：
    a. 按一下**匯出為建置區塊**。
    b. 鍵入此建置區塊的唯一名稱。
    c. 按一下**儲存**。
12. 在「群組」窗格中，選取您要爲其指派此規則的群組的勾選框。
13. 在**附註**欄位中，鍵入您要爲此規則包含的附註，然後按**下一步**。
14. 在「規則回應」頁面上，按一下**電子郵件**，然後輸入接收通知的電子郵件位址。 如需事件規則的其他回應參數的相關資訊，請參閱事件、流程和共用規則回應頁面參數。
15. 按**下一步**。
16. 如果規則正確，請按一下**完成**。

在 X-Force Exchange 中尋找 IP 位址和 URL 資訊

在 IBM Security QRadar 中使用右鍵功能表選項查閱 IBM Security X-Force Exchange 上找到的 IP 位址和 URL 相關資訊。您可以使用您的 QRadar 搜尋、攻擊和規則中的資訊，進一步研究或是將 IP 位址或 URL 的相關資訊新增至 X-Force Exchange 集合。

關於這項作業

當您研究安全問題時，可以提出公用或專用資訊以追蹤集合中的資料。

集合 (collection) 是一個儲存庫，您可以在其中儲存在調查期間所找到的資訊。 您可以使用集合來儲存 X-Force Exchange 報告、註解或任何其他內容。 X-Force Exchange 報告同時包含它儲存時的報告版本，以及報告現行版本的鏈結。 集合還包含一個具有 wiki 樣式記事本的區段（時間表），您可以在其中新增與集合相關的註解。

如需 X-Force Exchange 的相關資訊，請參閱 X-Force Exchange (https://exchange.xforce.ibmcloud.com/)。

程序

1. 若要從 X-Force Exchange 查閱 QRadar 中的 IP 位址，請遵循下列步驟：
    a. 選取**日誌活動** 或**網路活動**標籤。
    b. 用滑鼠右鍵按一下要在 X-Force Exchange 中檢視的 IP 位址，然後選取**其他選項 > 外掛程式選項 > X-Force Exchange 查閱**以開啓 X-Force Exchange 介面。
2. 若要從 X-Force Exchange 查閱 QRadar 中的 URL，請遵循下列步驟：
    a. 選取**攻擊**標籤，或是**攻擊**上提供的事件詳細資料視窗。
    b. 用滑鼠右鍵按一下要在 X-Force Exchange 中查閱的 URL，然後選取**外掛程式選項 > X-Force Exchange 查閱**以開啓 X-Force Exchange 介面。

管理誤判

使用 X-Force Threat Intelligence 來管理規則觸發程式的靈敏度，以便可以減少網路中的誤判數目。使用誤判調整可防止事件及流程與攻擊產生關聯。

信任係數

X-Force 將 IP 信譽資料分類，並將 0 - 100 的信任係數值指派給該分類，其中 0 代表不信任，而 100 代表肯定。例如，X-Force 可能將來源 IP 位址分類成信任係數爲 75 的掃描 IP，75 是中等層次的信任。

如何輸入信任值？

在 QRadar 中的下列 X-Force 規則測試中輸入信任值：**當此主機內容被 X-Force 分類成這個種類，且信任值等於這個數量時**

設定信任值的準則

信任係數是其中一個主要工具，您可用來協助限制所觸發規則建立的攻擊數。您可以根據想要的保護層次，將信任值調整成最符合您網路環境的層次。

在 DMZ 中，您可能想要選擇一個更高的信任值，例如，95% 或更高，因爲您不需要調查此區域中的許多攻擊。使用這個信任層次，IP 位址很有可能符合列出的種類。如果 95% 肯定主機正在處理惡意軟體，則您需要瞭解它。

可降低網路的較安全區域（例如伺服器儲存區）的信任值。透過降低信任層次，可能會識別更多的威脅，而相應的調查工作會減少，因爲威脅與特定網路區段相關。

若要進行最佳誤判調整，請依區段來管理規則觸發程式。查看網路基礎架構並決定哪些資產需要高階保護，而哪些資產不需要。可針對不同的網路區段套用不同的信任值。使用建置區塊對常用測試進行分組，以便測試可用於規則中。

URL 型規則

您可以查看共用虛擬主機作業網站中的誤判，因爲一個網站可能負責處理合法的內容，而同一 IP 位址中的另一個網站則負責處理惡意軟體。在共用虛擬主機作業設定中，URL 資訊很有用，因爲 URL 是更具體的指示器，指示所要傳輸的資料。URL 型規則可能比 IP 型規則更加精確。

針對 URL 型規則，您必須建立自訂事件內容來從有效負載擷取 URL。

如需調整誤判的相關資訊，請參閱《*調整手冊*》。

第 14 章 報告管理

您可以使用**報告**標籤來建立、編輯、配送及管理報告。

詳細且彈性的報告選項可滿足您各種管制標準，如 PCI 規範。

您可以建立自己的自訂報告或使用預設報告。您可以將預設報告予以自訂和品牌再造，以及將這些報告配送給其他使用者。

如果您的系統包括許多報告，**報告**標籤可能需要較長的時段來重新整理。

註：如果您在執行的是 Microsoft Exchange Server 5.5，以電子郵件郵寄報告的主旨行中可能會顯示無法使用的字型字元。 若要解決此問題，請下載並安裝 Microsoft Exchange Server 5.5 的 Service Pack 4。 如需相關資訊，請聯絡 Microsoft 支援。

時區考量

若要確保「報告」功能使用正確的日期和時間來報告資料，您的階段作業必須與您的時區同步。

在安裝及設定 QRadar 產品期間，系統已配置時區。 請與您的管理者核對，確保 QRadar 階段作業與您的時區同步。

報告標籤許可權

管理使用者可以檢視其他使用者所建立的所有報告。

非管理使用者只能檢視他們所建立的報告或是其他使用者所共用的報告。

報告標籤參數

報告標籤顯示預設和自訂報告清單。

從**報告**標籤中，您可以檢視關於報告範本的統計資訊、在報告範本上執行動作、檢視產生的報告、刪除產生的內容。

如果報告不指定間隔排程，則您必須手動產生報告。

您可以將滑鼠點在任何報告上，在工具提示中預覽報告摘要。 摘要指定報告配置以及報告產生的內容類型。

報告佈置

報告可以由數個資料元素組成，且可以用各種樣式（如表格、折線圖、圓餅圖及長條圖）代表網路及安全資料。

選取報告佈置時，請考量您要建立的報告類型。 例如，不要爲顯示許多物件的圖形內容選擇小圖表儲存器。 每個圖形都包含圖註及衍生內容的網路清單；請選擇足夠大的儲存器以保存資料。 若要預覽每個圖表顯示資料的方式，請參閱圖形類型。

圖表類型

建立報告時，您必須爲要包含在報告中的每個圖表選擇圖表類型。

圖表類型可判定產生的報告呈現資料及網路物件的方式。 您可以使用數個性質建立資料圖表，及在單一產生的報告中建立圖表。

您可以使用下列任何類型的圖表：

- **無** - 使用此選項在報告中顯示空儲存器。 在報告中建立空格時，此選項可能很有用。如果您對任何儲存器選取**無**選項，該儲存器無需進一步配置。
- **資產漏洞** - 使用此圖表來檢視部署中定義的每個資產的漏洞資料。您可以在 VA 掃描偵測到漏洞時產生「資產漏洞」圖表。 在安裝 IBM Security QRadar Vulnerability Manager 之後，此圖表可用。
- **連線** - 只有在您已購買 IBM Security QRadar Risk Manager 及獲得其授權時，才顯示此圖表選項。如需相關資訊，請參閱 *IBM Security QRadar Risk Manager User Guide*。
- **裝置規則** - 只有在您已購買 IBM Security QRadar Risk Manager 及獲得其授權時，才顯示此圖表選項。如需相關資訊，請參閱 *IBM Security QRadar Risk Manager User Guide*。
- **裝置未用的物件** - 只有在您已購買 IBM Security QRadar Risk Manager 及獲得其授權時，才顯示此圖表選項。如需相關資訊，請參閱 *IBM Security QRadar Risk Manager User Guide*。
- **事件/日誌** - 使用此圖表來檢視事件資訊。 您可以從**日誌活動**標籤，根據已儲存搜尋中的資料製作圖表。您可以自訂要顯示在所產生報告中的資料。 您可以配置圖表，以繪製可配置時段中的資料。 此功能可協助您偵測事件趨勢。 如需已儲存的搜尋的相關資訊，請參閱資料搜尋。
- **日誌來源** - 使用此圖表來匯出或報告日誌來源。 選取要出現在報告中的日誌來源及日誌來源群組。依報告直欄對日誌來源進行排序。 包括定義的時段內未報告的日誌來源。 包括特定時間建立的日誌來源。
- **流程** - 使用此圖表來檢視流程資訊。您可以從「網路活動」標籤，根據已儲存搜尋中的資料製作圖表。這可讓您自訂要顯示在所產生報告中的資料。您可以使用已儲存的搜尋配置圖表，以繪製可配置時段中的流程資料。此功能可協助您偵測流程趨勢。如需已儲存的搜尋的相關資訊，請參閱資料搜尋。
- **前幾個目的地 IP** - 使用此圖表來顯示您選取的網路位置中的前幾個目的地 IP。
- **前幾個攻擊** - 使用此圖表來顯示您選取的網路位置中目前發生的前幾個攻擊。
- **前幾個來源 IP** - 使用此圖表來顯示及排序攻擊您的網路或企業資產的前幾個攻擊來源（IP 位址）。
- **漏洞** - 只有在您已購買 IBM Security QRadar Vulnerability Manager 及獲得其授權時，才顯示「漏洞」選項。 如需相關資訊，請參閱 *IBM Security QRadar Vulnerability Manager User Guide*。

報告標籤工具列

您可以使用工具列對報告執行許多動作。

下表識別及說明「報告」工具列選項。

表 59. 報告工具列選項

選項	說明
分組	
管理群組	按一下**管理群組**可管理報告群組。 使用「管理群組」功能，您可以將報告組織爲功能群組。您可以與其他使用者共用報告群組。
動作	按一下**動作**可執行下列動作： • **建立** - 選取此選項可建立新的報告。 • **編輯** - 選取此選項可編輯選取的報告。 您也可以按兩下報告來編輯內容。 • **複製** - 選取此選項可複製或重新命名選取的報告。 • **指派群組** - 選取此選項可將選取的報告指派給報告群組。 • **共用** - 選取此選項可將選取的報告與其他使用者共用。 您必須具有管理專用權才能共用報告。 • **切換排程** - 選取此選項可將選取的報告切換爲「作用中」或「非作用中」狀態。 • **執行報告** - 選取此選項可產生選取的報告。若要產生多個報告，請按住 Ctrl 鍵並按一下要產生的報告。 • **在原始資料上執行報告** - 選取此選項可使用原始資料產生選取的報告。 如果您要在所需的累計資料可用之前產生報告，此選項很有用。 例如，如果要在自建立報告一整週經過之前執行每週報告，您可以使用此選項產生報告。 • **刪除報告** - 選取此選項可刪除選取的報告。若要刪除多個報告，請按住 Ctrl 鍵並按一下要刪除的報告。 • **刪除產生的內容** - 選取此選項可刪除選取列的所有產生的內容。 若要刪除多個產生的報告，請按住 Ctrl 鍵並按一下要刪除的產生報告。
隱藏互動式報告	選取此勾選框可隱藏非作用中的報告範本。 **報告**標籤會自動重新整理及僅顯示作用中的報告。 清除勾選框以顯示隱藏的非作用中報告。

表 59. 報告工具列選項 (繼續)

選項	說明
搜尋報告	在**搜尋報告**欄位中鍵入搜尋準則，然後按一下**搜尋報告**圖示。對下列參數執行搜尋，以判定與您指定的準則相符的內容。 • 報告標題 • 報告說明 • 報告群組 • 報告群組 • 報告作者使用者名稱

圖形類型

每種圖表類型支援您可以用於顯示資料的各種圖形類型。

網路配置檔可判定圖表用於描述網路資料流量的顏色。 使用唯一的顏色描述每個 IP 位址。下表提供在圖表中使用網路及安全資料的方式範例。 此表格說明適用於每種圖形類型的圖表類型。

表 60. 圖形類型

圖形類型	可用的圖表類型
折線圖	• 事件/日誌 • 流程 • 連線 • 漏洞
堆疊折線圖	• 事件/日誌 • 流程 • 連線 • 漏洞
長條圖	• 事件/日誌 • 流程 • 資產漏洞連線 • 連線 • 漏洞
水平長條圖	• 前幾個來源 IP • 前幾個攻擊 • 前幾個目的地 IP
堆疊長條圖	• 事件/日誌 • 流程 • 連線

表 60. 圖形類型 (繼續)

圖形類型	可用的圖表類型
圓餅圖	• 事件/日誌 • 流程 • 資產漏洞 • 連線 • 漏洞
表格	• 事件/日誌 • 流程 • 前幾個來源 IP • 前幾個攻擊 • 前幾個目的地 IP • 連線 • 漏洞 若要以表格顯示內容，您必須使用整頁寬度儲存器設計報告。
聚集表格	隨附於「資產漏洞」圖表。 若要以表格顯示內容，您必須使用整頁寬度儲存器設計報告。

下列圖形類型適用於 QRadar Log Manager 報告：

- 折線圖
- 堆疊折線圖
- 長條圖
- 堆疊長條圖
- 圓餅圖
- 表格圖

註：當您建立條欄和堆疊條欄圖表報告時，會以固定格式顯示圖註，在大部分情況下，條欄或條欄區段以色彩標示的標籤表示。如果您選取時間作爲 X 軸的值，則可以在 X 軸上建立時間間隔。

建立自訂報告

使用「報告」精靈來建立及自訂新報告。

開始之前

您必須具有適當的網路許可權，才能與其他使用者共用產生的報告。

如需許可權的相關資訊，請參閱 *IBM Security QRadar SIEM Administration Guide*。

關於這項作業

「報告」精靈會提供有關如何設計、排定及產生報告的逐步手冊。

此精靈使用下列主要元素來協助您建立報告：

- **佈置** - 每個儲存器的位置及大小
- **儲存器** - 精選內容的位置保留元。
- **內容** - 位於儲存器中的圖表定義

在建立每週或每月產生的報告之後，在產生的報告傳回結果之前，必須經過排定的時間。 對於已排程的報告，您必須等待排定的時段，以建置結果。 例如，每週搜尋需要七天來建置資料。 此搜尋將會在 7 天之後返回結果。

在您指定報告的輸出格式時，請考量所產生報告的檔案大小可能是 1-2 MB，具體情況視選取的輸出格式而定。 PDF 格式較小，不會耗用大量磁碟儲存體空間。

程序

1. 按一下**報告**標籤。
2. 從**動作**清單框中，選取**建立**。
3. 在「歡迎使用報告精靈！」視窗上，按**下一步**。
4. 選取下列其中一個選項：

選項	敘述
手動	依預設，報告產生 1 次。 您可以按需要的次數產生報告。
每小時	排定在每小時結束時產生報告。 使用前一個小時的資料。 從清單框中，選取開始及結束報告週期的時間範圍。 在此時間範圍內，每小時產生報告。 時間以半小時的增量提供。 **開始時間**及**截止時間**欄位的預設值爲 1:00 a.m。
每週	排定每週使用前一週的資料產生報告。 選取您要產生報告的日期。 預設值爲「星期一」。 從清單框中，選取開始報告週期的時間。 時間以半小時的增量提供。 預設值爲 1:00 a.m。
每月	排定每月使用前一月的資料產生報告。 從清單框中，選取您要產生報告的日期。 預設值爲本月的第一天。 選取產生報告週期的開始時間。 時間以半小時的增量提供。 預設值爲 1:00 a.m。

5. 在**容許手動產生此報告**窗格中，選取**是**或**否**。
6. 配置報告的佈置：
   a. 從**方向**清單框，選取**直印**或**橫印**，以作爲頁面方向。
   b. 選取「報告」精靈上顯示的六個佈置選項之一。
   c. 按**下一步**。
7. 指定下列參數的值：

參數	值
報告標題	此標題的長度最多可爲 100 個字元。 請勿使用特殊字元。
標誌	從清單框中，選取一個標誌。
頁數選項	從清單框中，選取頁數在報告上的顯示位置。 您可以選擇不顯示頁數。
報告分類	鍵入此報告的分類。 您可以鍵入的長度最多可爲 75 個字元。 您可以使用前導空格、特殊字元和雙位元組字元。 報告分類顯示在報告的標頭和標底中。 您可能希望將報告分類爲**機密**、**高度機密**、**敏感**或**內部**。

8. 配置報告中的每個儲存器：
   a. 從**圖表類型**清單框中，選取圖表類型。
   b. 在「儲存器詳細資料」視窗中，配置圖表參數。

      註：您還可以資產儲存的搜尋。 從**要使用的搜尋**清單框中，選取已儲存的搜尋。
   c. 按一下**儲存儲存器詳細資料**。
   d. 如果您選取了多個儲存器，請重複步驟 a 到 c。
   e. 按**下一步**。
9. 預覽「佈置預覽」頁面，然後按**下一步**。
10. 選取您要產生的報告格式的勾選框，然後按**下一步**。

    重要：「可延伸標記語言」僅適用於表格。
11. 選取報告的配送通道，然後按**下一步**。 選項包括下列配送通道：

選項	敘述
報告主控台	選取此勾選框以將產生的報告傳送至**報告**標籤。 **報告主控台**是預設配送通道。
選取應可以檢視產生的報告的使用者。	在您選取**報告主控台**勾選框之後，此選項會顯示。 從使用者清單中，選取您要授與檢視所產生報告的許可權的使用者。
選取所有使用者	僅在您選取**報告主控台**勾選框之後，此選項才會顯示。 如果您要授與所有使用者檢視所產生報告的許可權，請選取此勾選框。 您必須具有適當的網路許可權，才能與其他使用者共用產生的報告。
電子郵件	如果您要使用電子郵件配送產生的報告，請選取此勾選框。

選項	敘述
輸入報告配送電子郵件位址	僅在您選取**電子郵件**勾選框之後，此選項才會顯示。 鍵入每個所產生報告收件者的電子郵件位址；使用逗點區隔電子郵件位址清單。 此參數的字元數上限爲 255。 電子郵件收件者會從 no_reply_reports@qradar 收到此電子郵件。
將報告併入當作附件（僅限非 HTML）	僅在您選取**電子郵件**勾選框之後，此選項才會顯示。 選取此勾選框以將產生的報告作爲附件傳送。
併入報告主控台的鏈結	僅在您選取**電子郵件**勾選框之後，此選項才會顯示。 選取此勾選框，以將「報告主控台」的鏈結包含在電子郵件中。

12. 在「完成」頁面上，輸入下列參數的值。

選項	敘述
報告說明	鍵入此報告的說明。 說明會顯示在「報告摘要」頁面及產生的報告配送電子郵件中。
請選取您要包含此報告作為成員的任何群組	選取您要指派此報告至其中的群組。如需群組的相關資訊，請參閱報告群組。
您要現在執行報告嗎？	如果您要在精靈完成時產生報告，請選取此勾選框。 依預設，勾選框已選取。

13. 按**下一步**以檢視報告摘要。
14. 在「報告摘要」頁面上，選取摘要報告上可用的標籤以預覽報告配置。

結果

報告會立即產生。 如果在精靈的最後頁面上您已清除**您要現在執行報告嗎**勾選框，報告會儲存及在排定的時間產生。 報告標題是所產生報告的預設標題。如果您重新配置報告來輸入新的報告標題，報告會以新名稱儲存爲新報告；但是，原始報告保持不變。

編輯報告

使用「報告」精靈，您可以編輯任何預設值或自訂要變更的報告。

關於這項作業

您可以使用或自訂大量預設報告。 預設**報告**標籤會顯示報告清單。 每個報告會擷取及顯示現有的資料。

註：當您自訂排程報告以手動產生資料時，請先選取時間跨距**結束日期**，然後再選取**開始日期**。

程序

1. 按一下**報告**標籤。
2. 按兩下您要自訂的報告。
3. 在「報告」精靈上，變更參數以自訂要產生您所需內容的報告。

結果

如果您重新配置報告來輸入新的報告標題，報告會以新名稱儲存爲新報告；但是，原始報告保持不變。

檢視產生的報告

在**報告**標籤上，如果報告產生了內容，則會在**格式**欄中顯示圖示。 您可以按一下該圖示來檢視報告。

關於這項作業

如果報告產生了內容，則**產生的報告**欄會顯示清單框。 這個清單框會顯示所有產生的內容，並依報告的時間戳記進行組織。 最近的報告會顯示在清單頂端。如果報告沒有產生任何內容，則**產生的報告**欄中會顯示值**無**。

在**格式**欄中會顯示代表所產生之報告格式的圖示。

可以產生的報告格式如下：PDF、HTML、RTF、XML 和 XLS。

註：XML 與 XLS 格式僅適用於使用單個圖表表格格式（直印或橫印）的報告。

您只能檢視管理者授權您存取的報告。 管理使用者可以存取所有報告。

如果您使用 Mozilla Firefox Web 瀏覽器，並選取 RTF 報告格式，則 Mozilla Firefox Web 瀏覽器會開啓一個新的瀏覽器視窗。 這個新啓動的視窗是 Mozilla Firefox Web 瀏覽器配置所致，不會影響 QRadar。 您可以關閉視窗，並繼續您的 QRadar 階段作業。

程序

1. 按一下**報告**標籤。
2. 從清單框的**產生的報告**欄中，選取要檢視之報告的時間戳記。
3. 按一下要檢視之格式的圖示。

刪除產生的內容

在您刪除產生的內容時，已透過報告範本產生的所有報告都會刪除，但會保留報告範本。

程序

1. 按一下**報告**標籤。
2. 選取您要刪除所產生內容的報告。
3. 從**動作**清單框中，按一下**刪除產生的內容**。

手動產生報告

報告可以配置爲自動產生，但是，您也可以隨時手動產生報告。

關於這項作業

當產生報告時，「下次執行時間」欄會顯示下列三個訊息的其中一個：

- **產生中** - 正在產生報告。
- **已進入佇列（佇列中的位置）** - 報告已進入佇列等待產生。 訊息指示報告在佇列內的位置。 例如，第 1 個（共 3 個）。
- **（x 小時 x 分鐘 y 秒）** - 排定執行報告。 此訊息爲倒計時的計時器，它指定下一次執行報告的時間。

您可以選取**重新整理**圖示來重新整理視圖，包括**下次執行時間**欄中的資訊。

程序

1. 按一下**報告**標籤。
2. 選取您要產生的報告。
3. 按一下**執行報告**。

下一步

產生報告之後，您可以從「產生的報告」欄檢視產生的報告。

複製報告

若要建立非常類似於現有報告的報告，您可以複製要模型化的報告，然後自訂它。

程序

1. 按一下**報告**標籤。
2. 選取您要複製的報告。
3. 從**動作**清單框中，按一下**複製**。
4. 鍵入報告的新名稱，不含空格。

下一步

您可以自訂複製的報告。

共用報告

您可以與其他使用者共用報告。 當您共用報告時，會提供所選報告的副本給另一個使用者，以進行編輯或排程。

關於這項作業

使用者對共用報告所作的任何更新項目都不會影響該報告的原始版本。

您必須具有管理專用權才能共用報告。 另外，若要容許新使用者檢視和存取報告，管理使用者必須與新使用者共用所有必要的報告。

您只能與具有適當存取權的使用者共用報告。

程序

1. 按一下**報告**標籤。
2. 選取您要共用的報告。
3. 從**動作**清單框中，選取**共用**。
4. 從使用者清單中，選取要與其共用報告的使用者。

在報告上印品牌

若要在報告上印品牌，您可以匯入標誌及特定的影像。若要以自訂標誌在報告上印品牌，您必須先上傳並配置標誌，然後再開始使用「報告」精靈。

開始之前

確保您要使用的圖形爲白色背景的 144 x 50 像素。

若要確保瀏覽器顯示新的標誌，請清除瀏覽器快取。

關於這項作業

如果您支援多個標誌，則報告品牌行銷對於您的企業是有助益的。 上傳影像時，影像會自動另存爲「可攜式網路圖形 (PNG)」。

當上傳新影像，並將該影像設定爲預設影像時，新的預設影像不會套用至先前產生的報告。 要更新先前產生的報告上的標誌，需要從報告手動產生新內容。

如果您上傳的影像長度大於報告標頭可以支援的長度，則影像會自動調整大小以合配標頭；此高度大約爲 50 個像素。

程序

1. 按一下**報告**標籤。
2. 在導覽功能表上，按一下**品牌行銷**。
3. 按一下**瀏覽**以瀏覽系統上的檔案。
4. 選取包含您要上傳的標誌的檔案。 按一下**開啓**。
5. 按一下**上傳影像**。
6. 選取您要用作預設值的標誌，然後按一下**設定預設影像**。

報告群組

您可以將報告排序到功能群組。 如果您將報告分類到群組，就可以有效編排及尋找報告。

例如，您可以檢視與 Payment Card Industry Data Security Standard (PCIDSS) 規範相關的所有報告。

依預設，**報告**標籤會顯示所有報告清單，但是，您可以將報告分類爲群組，如：

- 相符性
- 執行程式
- 日誌來源

- 網路管理
- 安全
- VoIP
- 其他

建立新報告時，您可以將報告指派給現有的群組或建立新群組。 您必須具有建立、編輯或刪除群組的管理存取權。

如需使用者角色的相關資訊，請參閱 *IBM Security QRadar SIEM Administration Guide*。

建立報告群組

您可以建立新群組。

程序

1. 按一下**報告**標籤。
2. 按一下**管理群組**。
3. 使用導覽樹狀結構選取您要在其中建立新群組的群組。
4. 按一下**新建群組**。
5. 輸入下列參數的值：
   - **名稱** - 鍵入新群組的名稱。此名稱的長度最多可爲 255 個字元。
   - **說明** - 選用項目。 鍵入此群組的說明。 此說明的長度最多可爲 255 個字元。
6. 按一下**確定**。
7. 若要變更新群組的位置，請按一下新群組，然後將資料夾拖曳至導覽樹狀結構上的新位置。
8. 關閉「報告群組」視窗。

編輯群組

您可以編輯報告群組，以變更名稱或說明。

程序

1. 按一下**報告**標籤。
2. 按一下**管理群組**。
3. 從導覽樹狀結構中，選取您要編輯的群組。
4. 按一下**編輯**。
5. 根據需要更新參數的值：
   - **名稱** - 鍵入新群組的名稱。此名稱的長度最多可爲 255 個字元。
   - **說明** - 選用項目。 鍵入此群組的說明。 此說明的長度最多可爲 255 個字元。此欄位是選用項目。
6. 按一下**確定**。
7. 關閉「報告群組」視窗。

共用報告群組

您可以與其他使用者共用報告群組。

開始之前

您必須具有管理權限才能與其他使用者共用報告群組。

如需許可權的相關資訊，請參閱 *IBM Security QRadar SIEM Administration Guide*。

您無法使用「內容管理工具 (CMT)」來共用報告群組。

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

關於這項作業

在「報告群組」視窗中，共用使用者可以在報告清單中看到報告群組。

使用者對共用報告群組所作的任何更新項目都不會影響該報告的原始版本。 只有擁有者才能刪除或修改。

當使用者複製或執行共用報告時，會建立報告的副本。 使用者可以在複製的報告群組中編輯或排定報告。

群組共用選項會置換爲群組中的報告所配置的舊報告共用選項。

程序

1. 按一下**報告**標籤。
2. 在**報告**視窗上，按一下**管理群組**。
3. 在**報告群組**視窗上，選取要共用的報告群組，然後按**共用**。
4. 在**共用選項**視窗上，請選取下列一項。

選項	敘述
預設值（從母項繼承）	不共用報告群組。 任何複製的報告群組或產生的報告都將保留在使用者的報告清單中。 群組中的每一個報告都將被指派已配置的任何母項報告共用選項。
與每個人共用	與所有使用者共用報告群組。
與符合下列準則的使用者共用...	與特定的使用者共用報告群組。 **使用者角色** 從使用者角色清單中選取，並按新增圖示 (+)。 **安全設定檔** 從安全設定檔清單中選取，並按新增圖示 (+)。

5. 按一下**儲存**。

結果

在「報告群組」視窗中，共用使用者可以在報告清單中看到報告群組。 產生的報告會根據安全設定檔的設定來顯示內容。

將報告指派給群組

您可以使用**指派群組**選項將報告指派給其他群組。

程序

1. 按一下**報告**標籤。
2. 選取您要指派給群組的報告。
3. 從**動作**清單框中，選取**指派群組**。
4. 從**項目群組**清單中，選取您要指派給此報告的群組的勾選框。
5. 按一下**指派群組**。

將報告複製到其他群組

使用**複製**圖示來將報告複製到一個以上報告群組。

程序

1. 按一下**報告**標籤。
2. 按一下**管理群組**。
3. 從導覽樹狀結構中，選取您要複製的報告。
4. 按一下**複製**。
5. 選取您要複製報告至其中的群組。
6. 按一下**指派群組**。
7. 關閉「報告群組」視窗。

移除報告

使用**移除**圖示來從群組移除報告。

關於這項作業

當您從群組移除報告時，報告仍然存在於**報告**標籤上。 報告不會從系統中移除。

程序

1. 按一下**報告**標籤。
2. 按一下**管理群組**。
3. 從導覽樹狀結構中，導覽至包含您要移除之報告的資料夾。
4. 從群組清單中，選取您要移除的報告。
5. 按一下**移除**。
6. 按一下**確定**。
7. 關閉「報告群組」視窗。

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，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。 本文件在提及 IBM 的產品、程式或服務時，不表示或暗示只能使用 IBM 的產品、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 對該網站並不提供任何保證。 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。

本文件所提及之非 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 International Business Machines Corp. 在世界許多管轄區註冊的商標或註冊商標。其他產品及服務名稱可能是 IBM 或其他公司的商標。IBM 商標的最新清單可在 Web 的 "Copyright and trademark information" 中找到，網址爲 www.ibm.com/legal/copytrade.shtml。

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。

UNIX 係 The Open Group 在美國及/或其他國家或地區之註冊商標。

Java 和所有以 Java 爲基礎的商標及標誌是 Oracle 及（或）其子公司的商標或註冊商標。

其他公司、產品及服務名稱可能是第三者的商標或服務標誌。

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 216 頁的『六劃』 第 216 頁的『七劃』 第 216 頁的『八劃』 第 216 頁的『九劃』 第 216 頁的『十劃』 第 217 頁的『十一劃』 第 217 頁的『十二劃』 第 218 頁的『十三劃』 第 218 頁的『十四劃』 第 219 頁的『十七劃』 第 219 頁的『十八劃』 第 219 頁的『十九劃』 第 219 頁的『A』 第 219 頁的『C』 第 219 頁的『D』 第 219 頁的『F』 第 220 頁的『H』 第 220 頁的『I』 第 220 頁的『L』 第 220 頁的『M』 第 220 頁的『N』 第 220 頁的『O』 第 220 頁的『Q』 第 220 頁的『R』 第 220 頁的『S』 第 220 頁的『T』 第 221 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，在該間隔結束時，事件處理器必須將所有已擷取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

激增 (burst)
送入事件或流程速率突然劇增，使授權流程或事件速率超出限制。

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)
遠離主要站台並從事件控制器接收事件或資料流程的裝置。

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。

〔三劃〕

下載 PCAP 資料檔 81
下載 PCAP 檔案 82
大量載入
  分析事件和流程 187
  歷程關聯 187
工具列 63
工具列功能 39
已儲存的搜尋準則 18

〔四劃〕

內容
  修改自訂 161
  複製自訂 162
內容窗格 108
內容類型 157
分組事件參數 72
分組事件選項 72
分離儀表板項目 26
手動產生報告 206
支援的版本
  Web 瀏覽器 6
文件模式
  Internet Explorer Web 瀏覽器 7
日誌來源 70
日誌活動 12, 16, 17, 24, 27, 63, 78, 79, 125, 127, 129, 151, 152, 153, 155, 157, 165
  搜尋準則 133
  概觀 63
日誌活動儀表板項目 19
日誌活動標籤 9, 12, 63, 67, 68, 70, 72, 78, 80, 82, 129

〔五劃〕

主控台時間 15
主機 9
功能 166
右鍵功能表 67, 87
右鍵功能表選項 110
未剖析的事件資料 70
未處理的事件資料 70
正規化事件 68
正規化流程 88, 89
正規表示式內容類型 157
目的地 IP 位址 29

〔六劃〕

共用規則 166
共用報告 206
共用報告群組 209
列印資產設定檔 109
各種模式下的流程清單 94
名詞解釋 215
多個儀表板 17
安全 17
安全異常狀況 5
安全憑證 5
自訂內容 162
自訂事件及流程內容 157
自訂規則 165
自訂規則精靈 11, 23
自訂報告 201
自訂儀表板 17, 20, 24
自訂儀表板項目 18

〔七劃〕

串流事件 67
串流流程 88
串流模式 88
伺服器 9
刪除規則 173
刪除搜尋 153
刪除資產 121
刪除資產設定檔 120
刪除儀表板 27
即時 67
即時（串流） 12
快速過濾器 129
「我的攻擊」頁面 30
我的攻擊標籤 142
攻擊 17, 29, 30, 32, 36, 78, 129, 153, 155, 165
  指派給使用者 37
  歷程關聯 189
攻擊保留 35
攻擊參數 42
攻擊規則 166
攻擊許可權 29
攻擊項目 18
攻擊搜尋 142
攻擊搜尋群組 154
攻擊摘要 37
攻擊管理 29
攻擊儀表板項目 18
攻擊標籤 9, 12, 29, 33, 34, 35, 36, 38, 39, 42, 147, 148, 149, 150
更新使用者詳細資料 15
更新的攻擊數 20
系統 17
系統時間 15
系統通知 11, 27
系統通知儀表板項目 23
系統摘要儀表板項目 20

〔八劃〕

事件 78, 127, 129
事件和流程搜尋 129
事件清單 75
事件處理器 88
事件處理器結果 67
事件規則 166
事件搜尋群組 153, 154
事件詳細資料 77
事件詳細資料工具列 77
事件詳細資料工具列功能 77
事件詳細資料頁面 75
事件過濾器資訊 110
事件說明 75
事件數 20
依目的地 IP 分組的攻擊 32
依目的地 IP 頁面 148
依來源 IP 分組的攻擊 31
依種類分組的攻擊 31
依網路分組的攻擊 32
依網路頁面 149
使用者介面 9
使用者介面標籤 9, 10
使用者名稱 7, 14
使用者資訊 15
來源 IP 位址 29
來源 IP 頁面 147
取消搜尋 152
「所有攻擊」頁面 30
所有攻擊標籤 142
服務 109
服務窗格 108
狀態列 67, 88
表格 17
保護攻擊 35
前一分鐘（自動重新整理） 12

〔九劃〕

威脅 17
建立自訂規則 168
建立規則群組 173
建立報告 10
建立搜尋群組 153
建立新的搜尋群組 119, 154
建置區塊 166
  編輯 175
指定要檢視的資料物件數目 25
指定圖表類型 25
流程 85, 127, 129
流程規則 166
流程搜尋 18
流程搜尋群組 153, 154
流程群組 94
流程詳細資料 89, 94
流程詳細資料工具列 97
流程過濾器準則 87
流程數 20, 134
相符性 17
計算內容 159
計算的內容類型 157
重要詞彙 29
重新命名儀表板 26
重新整理資料 12
風險原則窗格 108
風險監視儀表板 20
  建立 20
風險管理
  監視風險變更 22
  監視原則合規性 20
風險管理程式儀表板
  建立 22
風險標籤 20

〔十劃〕

修改事件對映 78
套件窗格 108
時間序列圖表 125
訊息功能表 11
配送報告 10
配置及管理系統 10
配置及管理使用者 10
配置及管理網路、外掛程式和元件 10
配置日誌活動 25
配置頁面大小 17
配置連線 25
配置資料 10
配置圖表 127
配置網路活動 25
配置儀表板項目 25

〔十一劃〕

停用規則 172
動作 33
執行子搜尋 151
密碼 7
將攻擊標示爲追蹤 38
將項目指派給群組 174
將項目複製到群組 174
從群組移除已儲存的搜尋 155
從儀表板移除項目 26
控制項 10
授權金鑰 5
排序表格中的結果 12
排除選項 36
排程搜尋
  事件數 134
  搜尋 134
  儲存的搜尋 134
啓用規則 172
現行威脅層次 24
產品窗格 108
異常偵測規則 165, 170
異常偵測規則精靈 170
移除已儲存的搜尋 120
移除群組 120, 155
移除圖示 120
第三方掃描程式 108
組織儀表板項目 17
規則 165, 166
  回應 167
  停用 172
  啓用 172
  編輯 172
  複製 172
  檢視 168
  X-Force Exchange 192, 195
規則回應 178
規則頁面工具列 177
規則參數 176
規則許可權 165
規則測試 187
規則群組
  建立 173
  檢視 173
規則群組管理 173
規則管理 165, 171
許可權
  自訂內容 157
軟體驅動裝置 10
通知訊息 23
連線搜尋項目 20

〔十二劃〕

最近產生的報告 19
單一事件詳細資料 75
報告 16, 17
  編輯 204
  歷程關聯 189
  檢視 205
報告佈置 197
報告群組 209
報告標籤 10, 12, 199
測試 166
登入資訊 7
開始時間 187

〔十三劃〕

匯入資產 121
匯入資產設定檔 120
匯出至 CSV 98
匯出至 XML 98
匯出攻擊 36
匯出事件 82
匯出流程 98
匯出資產 122
匯出資產設定檔 120
搜尋 119, 129
  複製到群組 155
搜尋攻擊 29, 142, 147, 148, 149
搜尋結果
  刪除 153
  取消 152
  管理 152
搜尋結果數目 88
搜尋準則
  日誌活動標籤 151
  可用的已儲存 151
  刪除 151
  儲存 133
搜尋群組
  建立 154
  管理 153
  編輯 155
  檢視 153
搜尋群組視窗 153
搜尋資產 109
搜尋資產設定檔 116
新搜尋 119
新儀表板 24
新增功能
  使用手冊概觀 1
新增事件項目 27
新增附註 33
新增流程搜尋項目 27
新增特性
  使用手冊概觀 1

新增項目 18, 27
新增資產 109, 113
新增過濾器 151
新增儀表板項目 17
概觀
RESTful API 7
溢位記錄 88
群組
刪除 175
刪除項目 175
指派項目 174
移除 155
編輯 174
複製項目 174
裝置時間 187
裝置層次許可權 29
解除保護攻擊 36
資料搜尋 129
資產 9, 16, 17
資產名稱 109
資產設定檔 108, 111, 113, 118, 119, 120, 121, 122
資產設定檔頁面 109, 122
資產設定檔頁面參數 108
資產搜尋頁面 116
資產搜尋群組 118
資產漏洞 122
資產標籤 9, 108, 109, 110, 111, 113, 118, 119, 120, 121
過去 24 小時內的活動摘要 20
電子郵件通知 37
預設登入資訊 7
預設標籤 9

〔十四劃〕

圖形類型 200
圖表物件 126
圖表概觀 125
圖表圖註 126
圖表管理 125
圖表類型 198
對攻擊的動作 33
對映事件 78
旗標 23
漏洞 108, 109
漏洞窗格 108
漏洞詳細資料 122
漏洞管理儀表板 23
監視 85
監視攻擊 30, 31, 33
監視事件 19
監視網路 85
管理報告 10, 199
管理搜尋結果 152, 153
管理搜尋群組 150, 153
管理群組 120
管理網路 109
管理標籤 10, 30
網路 17, 32
網路介面窗格 108
網路活動 12, 16, 17, 18, 24, 27, 85, 88, 89, 125, 127, 129, 133, 151, 152, 153, 155, 157, 165
網路活動監視 88
網路活動標籤 9, 12, 85, 87, 88, 91, 97, 98, 129
網路活動標籤工具列 85
網路管理者 ix
網際網路威脅資訊中心 24
網際網路威脅層次 24
維護自訂規則 165
聚集 CVSS 評分 109
誤判 79, 97, 108
說明 16
說明內容 16

〔十五劃〕

儀表板 27
儀表板項目 27
儀表板管理 17
儀表板標籤 9, 11, 17, 18, 19, 20, 24, 26, 27
影像
上傳 207
報告
印品牌 207
播放資料 12
暫停資料 12
標籤 9
編輯建置區塊 175
編輯搜尋群組 119, 155
編輯群組 174, 208
編輯資產 113
線上說明 16
複製已儲存的搜尋 120, 155
複製規則 172
複製報告 206
調查 85
調查日誌活動 63
調查攻擊 9
調查事件 19, 29
調查事件日誌 9
調查流程 9, 29
調查資產 109
調查網路活動 85
調整直欄大小 16
調整誤判 79, 97

〔十六劃〕

導覽 QRadar SIEM 5
導覽功能表 30
歷程關聯
攻擊 189
建立設定檔 188
規則處理 187
開始時間 187
裝置時間 187
過去的執行的相關資訊 189

〔十七劃〕

儲存事件及流程搜尋準則 67
儲存搜尋準則 150
儲存準則 118, 150
儲存資產搜尋準則 118
應用程式 17
檢視 PCAP 資料 81
檢視分組事件 72
檢視分組流程 91
檢視自訂規則 165
檢視串流事件 67
檢視串流流程 88
檢視系統通知 27
檢視訊息 11
檢視規則群組 173
檢視搜尋群組 118, 153
檢視資產 109
檢視資產設定檔 111
檢視與事件相關聯的攻擊 78
隱藏攻擊 34

〔十八劃〕

瀏覽器模式
Internet Explorer Web 瀏覽器 7
簡介 ix

〔十九劃〕

關閉攻擊 34

〔二十三劃〕

顯示在新視窗中 26
顯示清單框 72, 91
顯示項目 23
顯示儀表板 17, 24, 26, 27

I

IBM Security QRadar Risk Manager 10
ID 109

IP 位址 13, 109

P

Packet Capture (PCAP) 資料 80
PCAP 資料 80, 81
PCAP 資料直欄 80, 82

Q

QFlow 收集器 88
QID 78
QRadar
  X-Force Threat Intelligence 資訊來源整合 191
QRadar Vulnerability Manager 108

R

Regex 內容 158
RESTful API
  概觀 7

W

Windows 修補程式窗格 108

X

X-Force Exchange
  規則 192, 195
X-Force Threat Intelligence 資訊來源
  與 QRadar 搭配使用 191
  範例 192, 193

Printed in Taiwan