IBM Security QRadar Incident Forensics
版本 7.3.0

使用手册

IBM

附註

在使用本資訊及其所支援的產品之前，請閱讀第 35 頁的『聲明』中的資訊。

產品資訊

本文件適用於 IBM QRadar Security Intelligence Platform 7.3.0 版 及後續發行版，直至有本文件的更新版本替代為止。

目錄

使用 IBM Security QRadar Incident Forensics 的簡介

本手冊包含使用 IBM® Security QRadar® Incident Forensics 調查安全發生事件的相關資訊。

讀者對象

調查者從網路資料流量及 Forensics 儲存庫中的文件擷取資訊。 此資訊在調查安全發生事件時使用。

技術文件

若要在 Web 上尋找 IBM Security QRadar 產品說明文件，包括所有翻譯文件，請存取 IBM Knowledge Center(http://www.ibm.com/support/knowledgecenter/SS42VS/welcome)。

如需如何在 QRadar 產品檔案庫中存取更多技術文件的相關資訊，請參閱存取 IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644)。

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、產品及服務係設計為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為。

請注意：

使用本程式可能會與部分法律或法規相抵觸，包括那些與隱私權、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。

附註

IBM Security QRadar Incident Forensics 設計用於幫助公司改良其安全環境與資料。更專業地說，IBM Security QRadar Incident Forensics 設計用於幫助公司進行調查，及更充分的瞭解網路安全發生事件。 此工具容許公司建立索引，並搜尋擷取的網路封包資料 (PCAP)，以及包含可以將此類資料重新建構為其原始格式的功能。 此重新建構功

能可以重新建構資料與檔案，包括電子郵件訊息、檔案及圖片附件、VoIP 通話與網站。有關此程式的各項功能及如何配置的相關資訊，包含於程式的手冊及隨附的其他說明文件中。 使用本程式可能會涉及法律或規章。 包括與隱私權、資料保護、僱用及電子通訊與儲存相關的法律。 IBM Security QRadar Incident Forensics 必須以合法之目的並透過合法方式使用。客戶同意在使用本程式時負責遵守適用的法律、規章及原則。 被授權方代表它將取得或已取得合法使用 IBM Security QRadar Incident Forensics 所需的同意、許可權或授權。

第 1 章 QRadar Incident Forensics 7.3.0 版 中的使用者新增功能

IBM Security QRadar Incident Forensics 7.3.0 版 為正在執行回復的使用者建立「封包擷取 (PCAP)」裝置選擇。

可用於 QRadar Incident Forensics 回復的 PCAP 裝置選擇

若要在執行 QRadar Incident Forensics 回復時僅查看部署上 PCAP 裝置的資料流量，請選擇**自訂擷取裝置**。

進一步瞭解 PCAP 裝置選擇...

第 2 章 安全調查

使用 IBM Security QRadar Incident Forensics，您可以偵測新出現的威脅、判定主要原因及防止重複出現。 透過使用取證工具，您可以快速地將分析聚焦於起始威脅的人員、其執行方式及已受損項目。

作為取證調查者，您可以追蹤網路犯罪的逐步動作，並重新建構與安全發生事件相關的原始網路資料。

當組織第一次開始意識到威脅或潛在安全風險或標準違規時，您可以將目標設為評量範圍，識別所涉及實體及瞭解誘因。

您可以在不同類型調查（例如網路安全、內部分析、詐騙與不當使用及證據收集）的特定實務範例中，使用 IBM Security QRadar Incident Forensics 中的工具。

1. 回復並重新建構與 IP 位址之間的網路階段作業。
2. 您可以透過建立的事件來查詢屬性的種類，以收集證明。

   當您建立回復時，會建立事件。
3. 使用搜尋過濾器只擷取您感興趣的資訊。
4. 根據調查類型，選擇 forensics 工具來為您提供所需的證明。

可疑內容

您可疑使用搜尋以尋找任何您已知有關攻擊者或發生事件的環境定義元素或 ID。 如果您在搜尋中使用關鍵字，則將返回可疑的內容。部分可疑內容可能與調查相關。

資料旋轉

透過將搜尋結果傳回的內容顯示為快速鏈結，從而實現資料旋轉。 例如，如果您搜尋 "Tom"，則結果可能包括 Tom 撰寫的電子郵件、Tom 的會談及更多環境定義資訊。 當您按一下以檢視某個電子郵件時，每個資產或實體（例如附件或 Tom 使用的電腦 ID）都顯示為鏈結。 調查者可以使用撰寫鏈結來快速調查。

Digital Impression

使用 Digital Impression，可以查看資料，並根據頻率對映實體（例如 IP 位址、名稱及 MAC 位址）之間的關係。 您可以選取一個以上結果，以檢視關係的頻率及方向。

Surveyor

使用 Surveyor 以查看活動的時間表，以便您可以追溯攻擊。調查者會依時間順序重新建構階段作業和排序文件。

內容過濾

使用內容過濾，可以查看內容種類的子集（例如 WebMail、Pornography），以協助您在搜尋時移除雜訊或不相關內容。

網路安全調查

您可以使用 QRadar Incident Forensics 來偵測並調查將重要資產作為目標的惡意活動。您可以使用內建取證工具，協助您補救網路安全違背，並防止它再次發生。

使用 QRadar Incident Forensics 調查工具，以協助您找出事件發生方式、最小化其影響並執行您可以執行的每一個動作來防止另一個違規。

零容忍：識別攻擊的來源

在此實務範例中，組織收到警示，說明可疑違規。 它會探查以尋找攻擊的起始點，從而隔離來源。 組織必須隔離已受損實體，從而防止攻擊展開至組織的其他部分。

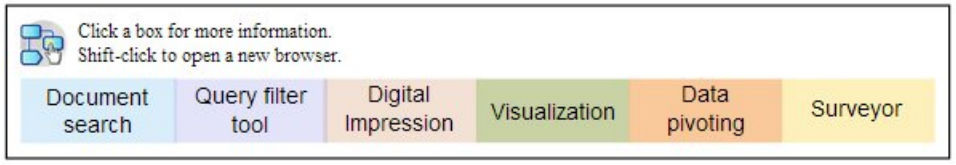
目標

為了解決這些調查中的問題，組織具有下列目標：

- 判定攻擊類型。
- 識別威脅的起始進入點。
- 取得惡意內容的詳細資料。
- 瞭解惡意內容如何從進入點散佈。

調查

使用**取證**標籤上的工具，可以協助您進行調查。



1. 使用開放式搜尋以搜尋與惡意內容相關聯的有症狀屬性。
2. 使用內容種類，以過濾掉與調查無關的內容。
3. 檢查產品標示的可疑內容。
4. 使用 Digital Impression 及視覺化，以探索惡意內容、嫌犯或目標的延伸關係。
5. 使用資料旋轉，並遵循資料鏈結以識別零容忍。
6. 使用 Surveyor 以查看活動的時間表，以便您可以追溯攻擊。

已受損系統

在此實務範例中，組織收到警示，說明進階網路攻擊技術（水坑攻擊、網路釣魚、暴力密碼破解或 SQL 注入）已讓一個以上系統受損。

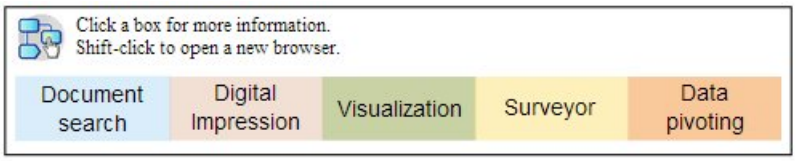
目標

為了解決這些調查中的問題，組織具有下列目標：

- 判定組織內受損的範圍。
- 瞭解每一個系統上受損的作業風險類型。
- 發現起始攻擊執行以避免清理活動及偵測的所有週邊動作。

調查

使用**取證**標籤上的工具，可以協助您進行調查。



1. 使用開放式搜尋以搜尋惡意內容或已受損資產。
2. 檢查產品標示的可疑內容。
3. 使用 Digital Impression 與「視覺化」，以探索已受損系統產生的實體關係。
4. 使用 Surveyor 以查看活動的時間表，以便您可以追溯攻擊。
5. 使用開放式搜尋、資料旋轉及可疑內容，來探索資料種類之間的不一致或可疑互動。

資料已洩漏給未獲授權的實體

在此實務範例中，組織收到警示，說明機密資料已洩漏給組織內未獲授權的實體或外部方。

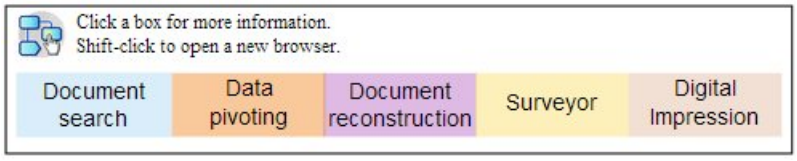
目標

為了解決這些調查中的問題，組織具有下列目標：

- 判定已洩漏資料的本質與數量。
- 瞭解所使用的技術。
- 發現嫌犯。
- 識別洩漏來源。

調查

使用**取證**標籤上的工具，可以協助您進行調查。



1. 使用開放式搜尋以搜尋已洩漏資料的 ID。
2. 檢查產品標示的可疑內容。
3. 透過檢閱資料重新建構，來檢閱已洩漏或正在洩漏資料的完整範圍。
4. 使用 Digital Impression 及視覺化以探索所有所涉及實體關係。
5. 使用 Surveyor 以查看活動的時間表，以便您可以追溯攻擊。
6. 使用開放式搜尋以探索資料洩漏的誘因。
7. 使用資料旋轉以尋找與其他可能洩漏資料的鏈結。

內部分析調查

使用 QRadar Incident Forensics，可以偵測存取的勾結、蓄意毀壞與錯誤使用。 識別嫌犯、識別合作者、識別已受損系統並記錄資料流失。

錯誤使用存取

在此實務範例中，組織收到警示，說明其一個以上員工正在錯誤使用認證，或用作代理人員以存取機密系統或資料，進行未獲授權的活動。

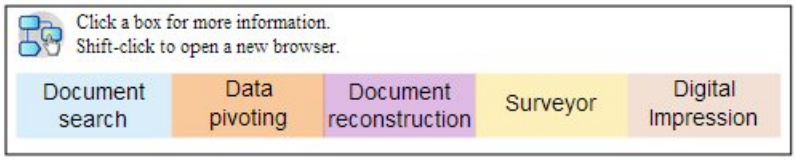
目標

為了解決這些調查中的問題，組織具有下列目標：

- 判定使用者身分。
- 解析誰或什麼正在使用未獲授權活動的身分。
- 瞭解錯誤使用存取的目標。
- 評量實體是否具有更多可能也錯誤使用的身分。

調查

使用**取證**標籤上的工具，可以協助您進行調查。



1. 使用開放式搜尋以搜尋正在存取機密系統或資料的身分。
2. 透過查看可以內容，執行開放式搜尋、資料旋轉及內容過濾，解析那些存取嘗試中哪些可疑。
3. 檢視正在存取之內容的資料重新建構。
4. 在 Surveyor 中追溯任何存取型樣並評估頻率。
5. 使用 Digital Impression 以顯示單一實體使用的別名。

勾結

在此實務範例中，組織收到警示，說明一個以上利害關係人正在彼此或與外部方勾結，從事對組織有害的活動。

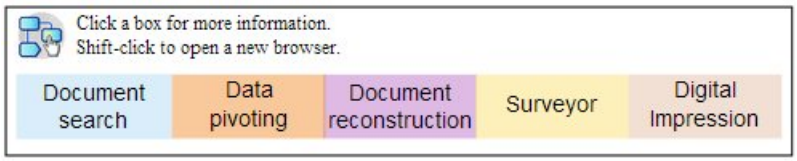
目標

為了解決這些調查中的問題，組織具有下列目標：

- 判定勾結實體。
- 瞭解合作者之間互動的本質和型樣。
- 發現位於方法下方的內容。
- 顯示方法的持續時間以瞭解風險範圍。

調查

使用**取證**標籤上的工具，可以協助您進行調查。



1. 使用開放式搜尋以搜尋所涉及實體的 ID。
2. 檢查產品標示的可疑內容。
3. 使用 Digital Impression、視覺化及內容過濾，以識別可能可疑的關係。
4. 使用 Surveyor 以追蹤所涉及實體的活動，從而取得互動的內容。
5. 透過檢閱已重新建構的文件，探索勾結的誘因。
6. 使用開放式搜尋及資料旋轉，以尋找勾結活動的開頭。

蓄意毀壞

在此實務範例中，組織收到警示，說明一個以上利害關係人正在嘗試毀壞作業。 利害關係人可能正用作代理人員。

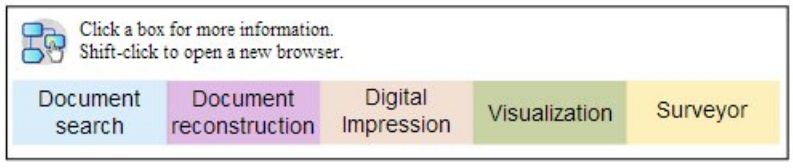
目標

為了解決這些調查中的問題，組織具有下列目標：

- 識別蓄意毀壞。
- 瞭解蓄意毀壞所使用的技術。
- 評量毀壞的影響與範圍。
- 精確找出蓄意毀壞利用的漏洞。

調查

使用**取證**標籤上的工具，可以協助您進行調查。



1. 使用開放式搜尋以搜尋蓄意毀壞的症狀。
2. 檢查產品標示的可疑內容。
3. 使用視覺化導覽、Digital Impression 及內容過濾以探索症狀，並偵測蓄意毀壞者的 ID。
4. 使用 Surveyor 以追蹤蓄意毀壞者的活動。
5. 使用資料重新建構以探索蓄意毀壞者角色與誘因。
6. 使用資料重新建構以檢閱虛擬毀壞者使用的內容。
7. 使用開放式搜尋、Surveyor 及可疑內容，以顯示啟用蓄意毀壞的已受損系統及程序。

詐騙與不當使用調查

使用 QRadar Incident Forensics，可以找到未獲授權的交易、未經認證的資源配置、通訊協定偏差及規避法律控制項。

未獲授權的交易

在此實務範例中，組織收到警示，說明未獲授權的交易導致對商業作業造成負面財務影響。

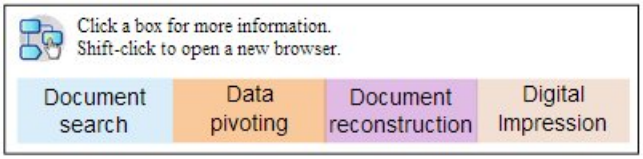
目標

為了解決這些調查中的問題，組織具有下列目標：

- 找到未獲授權的交易。
- 識別涉及並負責未獲授權交易的實體。
- 瞭解未獲授權交易的頻率與趨勢。
- 評量未獲授權交易的風險範圍。

調查

使用**取證**標籤上的工具，可以協助您進行調查。



1. 使用開放式搜尋以搜尋任何不一致或可疑交易。
2. 使用開放式搜尋與資料旋轉以搜尋那些交易的重複項。
3. 使用資料旋轉與 Digital Impression 以探索與可疑交易相關聯的實體。
4. 發現交易的內容，透過檢閱已重新建構文件來顯示定量值。

未經認證的資源配置

在此實務範例中，組織懷疑未經認證的資源配置，這可能導致對商業作業造成負面財務影響。

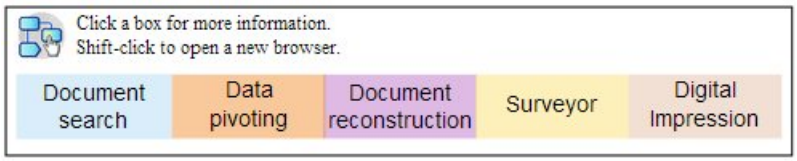
目標

為了解決這些調查中的問題，組織具有下列目標：

- 找到資源的錯誤配置。
- 識別涉及並負責資源錯誤配置的實體。
- 瞭解未經認證的資源配置的誘因。
- 評量錯誤配置資源的大小與範圍。

調查

使用**取證**標籤上的工具，可以協助您進行調查。



1. 將開放式搜尋用於與已配置資源相關聯的通訊。
2. 使用開放式搜尋、資料旋轉與 Digital Impression，以尋找進行未經認證之資源配置的實體 ID。
3. 透過檢閱已重新建構文件並使用視覺化，來處理評量目的所涉及的互動內容。
4. 使用 Surveyor 以追溯配置活動，從而瞭解錯誤配置資源的數量。

通訊協定偏差與規避法律控制項

在此實務範例中，組織收到警示，說明已規避商業、IT 通訊協定及法律控制項，這可能造成負面財務影響。

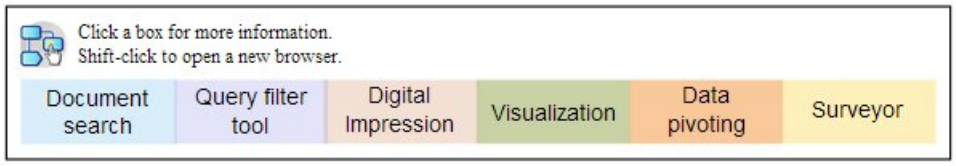
目標

為了解決這些調查中的問題，組織具有下列目標：

- 評量已規避的通訊協定或法律控制項。
- 精確找出參與此行為的實體。
- 瞭解這些實體的誘因。
- 評量這個錯誤行為的通用性。

調查

使用**取證**標籤上的工具，可以協助您進行調查。



1. 使用開放式搜尋以搜尋通訊協定或控制項控管的商業程序。
2. 使用開放式搜尋、資料旋轉及資料重新建構，與說明通訊協定與法律控制項的說明文件進行交互參照。
3. 使用內容過濾、開放式搜尋，以探索所規避通訊協定/控制項的特定實例。
4. 使用 Digital Impression、視覺化、資料旋轉及內容過濾，以尋找相關聯的實體 ID。
5. 使用 Surveyor 以追溯實體活動，從而探索可能的誘因。

證據收集調查

使用 QRadar Incident Forensics，可以評量組織中漏洞的風險，量化識別威脅或嫌犯的信任，以及精簡安全實務。

識別威脅中的信任

在此實務範例中，組織收到警示，說明某個威脅、惡意探索或漏洞。 為了證明可能取代一般商業作業的補救工作，他們可能想要量化任何相關聯風險的信賴區間。

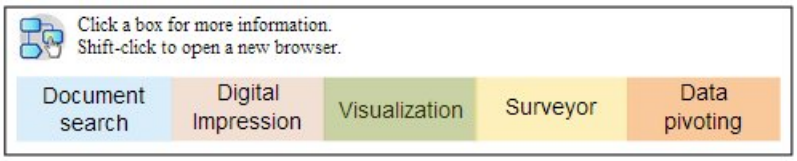
目標

為了解決這些調查中的問題，組織具有下列目標：

- 驗證安全風險的易損壞性。
- 判定是否有安全風險的證據。
- 評量安全風險的廣泛度與貨幣影響。
- 瞭解安全風險的本質

調查

使用**取證**標籤上的工具，可以協助您進行調查。



1. 使用開放式搜尋、可疑內容及資料旋轉，將潛在目標實體用作起始點，以搜尋威脅、惡意探索或漏洞。
2. 使用開放式搜尋及資料旋轉以編譯出現項目。
3. 使用開放式搜尋，以交互參照可能提供對影響參照的文件。
4. 使用 Digital Impression 及視覺化以識別受影響實體。
5. 使用 Surveyor 以分析與威脅或嫌犯相關聯的活動。

精簡安全實務

偵測新的與有風險的行為會促使組織評量現有安全實務是否足夠。 在次實務範例中，組織會探查以針對所面對風險評定其安全規則的有效性。

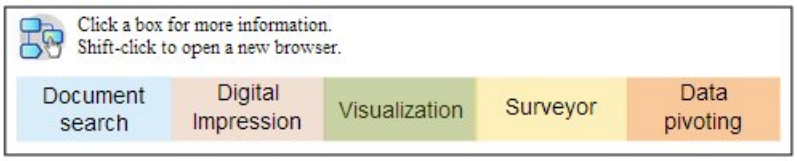
目標

為了解決這些調查中的問題，組織具有下列目標：

- 辨識新的或有風險的行為。
- 評量現有安全規則的效力。
- 瞭解由於動態作業而出現的安全間隙。
- 評估所提出安全實務的有效性。

調查

使用**取證**標籤上的工具，可以協助您進行調查。



1. 使用開放式搜尋，利用網域與組織知識，來搜尋新的或有風險的行為，例如針對行動使用者及基於雲端的服務。
2. 檢查可以內容，並使用 Surveyor 以與現有安全規則或實務交互參照這些行為。
3. 使用開放式搜尋、Surveyor、內容重新建構及視覺化，分析來自安全規則之警示的誤判頻率。
4. 使用開放式搜尋、Surveyor、內容重新建構、資料旋轉及視覺化，以探索現有安全規則或實務未偵測到的假性無侵害攻擊。

風險評量

在此實務範例中，說明某些漏洞、惡意探索或惡意行為的安全公告提示組織執行風險評量。 風險評量會判定組織是否易受損或已受損。

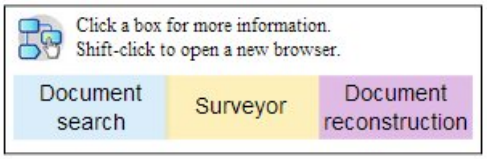
目標

為了解決這些調查中的問題，組織具有下列目標：

- 評量組織中已識別漏洞的顯示狀態。
- 偵測外部方的惡意顯示狀態。
- 發現任何受損的證據。
- 判定組織是否為惡意探索的受害者。
- 判定使用者身分。

調查

使用**取證**標籤上的工具，可以協助您進行調查。



1. 使用開放式搜尋以搜尋安全公告中指定之漏洞、惡意探索或其他惡意行為的特徵。
2. 使用開放式搜尋以交互參照研究或其他資料，從而衍生指示器。
3. 使用 Surveyor 以調查所識別之可能利用漏洞的互動。
4. 檢查產品標示的可疑內容。
5. 透過使用資料重新建構，檢閱進行潛在有風險互動的內容。
6. 使用 Surveyor 以追溯潛在有風險實體的活動。

第 3 章 forensics 調查入門

若要在 IBM Security QRadar Incident Forensics 中開始 forensics 調查，請使用**快速入門**功能表以導覽及過濾 forensics 儲存庫中的資料。此啟動程式包含預先定義的摘要查詢，您可用於開始搜尋或取得實體的關係。

若要開始，請遵循以下準則：

1. 開始 forensics 回復或從**攻擊**標籤上的攻擊中搜尋。
   - 如果您用滑鼠右鍵按一下攻擊或任何 IP 位址並執行 forensics 回復，則 forensics 會從擷取裝置擷取指定時間範圍內的原始擷取資料、解壓縮及重建文件，然後將結果新增至 forensics 儲存庫。
   - 如果您用滑鼠右鍵按一下攻擊或任何 IP 位址並執行 forensics 搜尋，會針對 IP 位址過濾及搜尋 forensics 儲存庫。然後，結果會顯示在 **Forensics** 標籤上的主要網格中。您可以建置查詢來精簡搜尋。

   QRadar Incident Forensics 接收搜尋要求時，它會處理封包擷取資料，並將其恢復為已傳送至預期的收件人的格式。例如，Microsoft Word 文件回復為 Word 檔案。Voice-over-IP 電話呼叫會回復為音訊檔案。然後，同時使用 meta 資料及檔案內容編製已回復檔案的索引，以使這些檔案可搜尋。
2. 在 **Forensics** 標籤上，按一下**快速入門**。

   執行回復或搜尋（而不是執行開放式搜尋及建置自己的查詢）之後，您可以使用 **Forensics** 標籤上**快速入門**功能表中預先定義的查詢，來快速開始調查。例如，您可以查看**可疑內容**種類，並執行其中一個查詢，如**實體警示**。可疑內容基於表示可疑活動的內容的預先定義規則集。實體警示會標示涉及中斷安全原則的可能惡意實體。

   內容分類及過濾功能有助於減少傳回的資料量
3. 從**網格**中，選取要查看的文件。

   QRadar Incident Forensics 會傳回依優先順序的搜尋結果。與在網際網路搜尋中搜尋引擎最佳化優先順序的方式相似，最頻繁出現的項目會顯示在清單頂部。

   您可以按一下鏈結及搜尋與文件相關聯的 meta 資料來開始旋轉資料。資料旋轉功能提供各種搜尋視圖及資料摘要。
4. 若要調查所有動作與資安事件之間的關係，請在文件視圖中選取鏈結，然後用滑鼠右鍵按一下**取得相關關係**。

   調查屬性之後，過濾透過連接實體收集的資訊。
5. 按一下**數位印記**，以追蹤身分軌跡及取得編譯的關聯集。

   數位印記是 meta 資料的索引，可透過追蹤惡意使用者軌跡來協助識別可疑攻擊者或內部欺詐者。在建置這些關係時，QRadar Incident Forensics 使用網路來源中的資料，如 IP 位址、MAC 位址及 TCP 埠與通訊協定。它可以尋找會談 ID 等資訊，及可以從文書處理或試算表應用程式讀取作者識別等資訊。數位印記可以透過將實體身分鏈結至其他使用者或實體的識別資訊，來協助發現關聯。

QRadar Incident Forensics 搜尋和書籤

調查者使用 IBM Security QRadar Incident Forensics 來從網路資料流量及文件擷取相關資料。

搜尋記錄並加上書籤

為了啟用直觀 forensics 活動，QRadar Incident Forensics 擷取封包資料，並吸收其他內容。 此技術提供搜尋驅動的資料探索、階段作業重新建構，以及 forensics 智能，來協助進行安全事件調查。

調查者使用粗部調查，然後繼續細部調整這些發現，以取得相關的最終結果集。 簡式的高層次方式是首先搜尋許多記錄，然後加上書籤。 然後，關注加上書籤的記錄，以識別最終記錄集。 判定哪種資料相關，並調整查詢，以包括或排除項目。 使用該資料來證明猜想。

在您開發新線索時，可以使用其他方法進行延續。 您可以使用視覺化及分析工具，來手動及自動評量結果的相關性。 您也可以使用改變的查詢，來取得相同問題的不同方面。

處理加上書籤的結果

當您搜尋對調查極為重要的結果時，可以為結果加上書籤，以便更深入檢驗及最終判定。 加書籤的數量需超過您認為所需的。 如果有疑問，請加上書籤。 您想要刪除無關資料，並關注您認為相關的資料。

在對您認為相關的結果集加上書籤之後，可以細部調整您的檢驗。

1. 透過視覺化與分析工具檢查每一個加上書籤的文件。
2. 將案例注意事項附加到文件中，然後對每一個文件與案例的相關性做出最終決策。
3. 如果記錄無關，請移除書籤。

   在調查過程中，您已識別儲存庫中的相關資料，且現在具有一組加上書籤的相關記錄。
4. 列印、匯出或處理相關記錄。

文件搜尋與調查

調查者可以搜尋與發生安全事件有關的線索或猜想相關的文件。

搜尋

調查者可以使用 forensic 儲存庫來擷取滿足所需性質的文件，而不必手動遍歷大規模的文件，而其中大部分與案例無關。 例如，在特定時段內產生的文件、與感興趣的主題相關的文件，或是由可疑攻擊者傳送或接收的文件。

搜尋可以是特定的。 例如，「尋找確切的字串 "Mission Alpha"」是特定的。 此外，搜尋可以通用。 例如，「尋找所有社會安全號，無論其是否在儲存庫中」更為通用。

搜尋可以是簡式，且僅基於一個準則。 複式搜尋結果必須滿足多個條件。 例如，尋找兩個可以攻擊者之間有關某個主題的所有電子郵件，以及排除包含附件的電子郵件是複式搜尋。 搜尋目的是快速並精確地將記錄減少為可管理的工作集。 使用較少的文件集以供調查者檢查，文件與案例高度相關。

Forensics 回復

若要從封包擷取裝置擷取封包擷取資料，可對一或多個 IP 位址或埠執行 Forensics 回復工作。

針對 IP 位址或埠執行回復

執行 Forensics 回復，以從擷取裝置擷取原始擷取資料。您可以針對多個 IP 位址或埠執行回復。如果您不輸入 IP 位址或埠，則會回復所有 TCP 和 UDP 資料流量。如果您輸入多個 IP 位址或埠，則必須使用逗點區隔它們。

在 QRadar 中用滑鼠右鍵按一下 IP 位址或埠，或在 Forensics 標籤上選取**執行回復**

圖示  來執行 Forensics 回復。

限制：因此，您一次可以輸入大約 7 個 IPv4 位址及 7 個埠，或最多 255 個字元。**IP 位址**與**埠**欄位與其他詞組結合，來建立過濾器字串。過濾器字串不能超過 255 個字元

重新執行回復

在 Forensics 標籤上，使用結果格線上的重新執行回復選項來執行之前建立的回復。例如，如果結果返回不完整的資料，請重新執行 Forensics 回復來包含不同的 IP 位址，或變更前一個執行回復工作中指定的時間範圍。

若要重新執行前一個 Forensics 回復工作，請按一下**重新執行此 Forensics 回復**。當您重新執行回復工作時，「Forensics 回復」頁面包含之前執行的值。您可以重新執行相同的回復，或變更自動產生的值。

您只能在完成工作、工作具有已完成、已取消或失敗狀態後重新執行回復。

Forensic 案例

案例為收集匯入的文件及封包擷取檔案的邏輯儲存器。

案例可以由管理者建立，或是有權建立案例的調查者建立。管理者建立案例，並將其指派給調查者。 調查者可以在從 IBM Security QRadar 中的任何 IP 位址擷取封包擷取資料時，建立新案例。

相關工作:

第 16 頁的『將 pcap 檔案與文件從外部系統上傳至取證案例』
您可以將外部資料上傳至特定案例。

集合

使用集合可對特定來源的相關資料進行分組，例如，封包擷取 (pcap) 資料檔案、PDF 或網路串流。

集合用來識別及管理相關資料的群組。您可以在調查完成時，快速刪除集合中的群組資料。

集合可以由管理者或調查者建立。 管理者建立集合，以便將資料手動載入 IBM Security QRadar Incident Forensics。 管理者還可以向案例新增集合。 調查者可以在從 IBM Security QRadar 中的任何 IP 位址起始擷取封包擷取資料時，新建集合。

對於集合與集合名稱，請考量下列規則：

- 集合名稱必須是唯一的。
- 案例包含一或多個集合。
- 集合可以新增至多個案例。
- 當調查者有兩個案例具有相同的集合時，搜尋結果返回重複的資料。
- 如果上傳新的 pcap 時，集合名稱不是唯一的，則會在上傳新的 pcap 之前刪除原始集合。

將 pcap 檔案與文件從外部系統上傳至取證案例

您可以將外部資料上傳至特定案例。

開始之前

管理者必須針對想要上傳外部檔案的使用者啟用安全 FTP 許可權。

關於這項作業

IBM Security QRadar Incident Forensics 可以從網路上的任何可存取目錄中匯入資料。資料可以使用許多格式，包括但不限於下列格式：

- 來自外部來源的標準 PCAP 格式檔案
- 文件，例如文字檔、PDF 檔、試算表及簡報
- 映像檔
- 來自應用程式的串流資料
- 來自外部 PCAP 來源的串流資料

您可以將多個檔案上傳至案例。

限制：案例名稱必須是唯一的。 您不能建立與現有案例具有相同名稱的案例。

程序

1. 在 FTP 用戶端中，執行下列步驟：
   a. 確保「傳輸層安全 (TLS)」選取為通訊協定。
   b. 新增 QRadar Incident Forensics 主機的 IP 位址。
   c. 建立使用所建立 QRadar Incident Forensics 使用者名稱與密碼的登入。
2. 連接至 QRadar Incident Forensics 伺服器，並建立新的目錄。
3. 若要以 FTP 傳輸 pcap 檔並予以儲存，請在為案例建立的目錄下，建立名為 `singles` 的目錄，並將 pcap 檔拖曳至該目錄。
4. 若要以 FTP 傳輸並非 pcap 檔的其他檔案類型並予以儲存，請在為案例建立的目錄下，建立名為 `import` 的目錄，並將檔案拖曳至該目錄。
5. 若要重新啟動 FTP 伺服器，請鍵入下列指令：

```
etc/init.d/vsftpd restart
```

6. 若要重新啟動將檔案從上傳區域移至 QRadar Incident Forensics 目錄的伺服器，請鍵入下列指令：

結果

您可以在**取證**標籤上的其中一個工具內查看案例。

Forensics 儲存庫查詢

調查者可指定他們希望從 forensics 資料庫擷取的文件性質。 使用多個查詢來尋找一組調查文件。

多重查詢及手動檢驗少量文件，較之在整個儲存庫中遍訪更為合適。 後續查詢與精簡查詢的構想經常在檢驗無關文件時產生。

增加查詢術語的數量及特殊性，可產生高度相關的結果集。 您的目標是定義足夠多能取得所需結果的術語，若有可能盡量將其特定化。搜尋準則中可以輸入任何數量的查詢術語。使用空格或布林運算子來分隔術語。 僅使用空格分隔的術語默示為布林邏輯 OR 運算子。 OR 運算子表示發現任何術語都是所需的。滿足最多搜尋詞彙的結果置於清單最上方，指示符合查詢術語的強度。

單個搜尋準則也叫作查詢術語。搜尋一般涉及多個查詢術語。 單個搜尋的查詢術語集也叫作查詢字串。 適應公式化查詢需要練習，但不會很難。 它僅涉及數個查詢術語，學習如何建立與無效化所需組合中的術語。 由於查詢字串儲存在 QRadar Incident Forensics 中，您可以在更好地學習資料之後繼續細部調整搜尋。

相關工作:

第 27 頁的『視覺化關係及關聯』
使用「視覺化」視窗來查看回復文件屬性之間的關係。例如，您可以檢查與特定電子郵件位址通訊的電子郵件位址。

開放式查詢術語

調查者可以在 **Forensics** 標籤上的搜尋準則欄位中直接輸入查詢術語，以搜尋確切的字串相符項。 您可以使用單個或多個單字查詢。

下表說明了可以使用的搜尋查詢類型。

表 *1.* 開放式查詢的類型

搜尋查詢類型	說明	範例
單字查詢	搜尋文件中的一個術語。	puppies
含萬用字元的單字查詢	搜尋符合查詢術語中間或結尾一或多個字元的相符項。 **限制：**萬用字元無法用作搜尋中的第一個字元。	te?t test* te*t
多字查詢	指定搜尋結果以查詢術語相關性順序返回。 同時包含兩個查詢術語的文件最先列出，接著列出僅包含其中一個查詢術語的文件。 僅包含一個查詢術語的文件將根據個別查詢術語的出現次數排列等級。	free puppies

表 1. 開放式查詢的類型 (繼續)

搜尋查詢類型	說明	範例
含雙引號的多字查詢	符合確切的字串。 同時包含兩個單字，但並非此順序及此近似性的文件將不會作為結果返回。 雙引號可以有效地將這兩個單字轉換成單個字串或查詢術語。 對於搜尋引擎，不會再將其看作兩個獨立單字。	"free puppies"
使用 AND 運算子的多個單字查詢	指定文件中必須同時存在這兩個查詢術語才能返回相符項。 查詢術語可使用任何順序，且彼此之間不必近似。	free AND puppies

Meta 資料標記

一般實體標記為容許調查者從相關文件快速擷取確切的結果集。

根據階段作業、文件或通訊協定的類型，Incident Forensic 索引中可以使用多類 meta 資料欄位。

當您指定 meta 資料標籤名稱時，它必須十分確切，且存在於 Forensic 儲存庫內。

下表列出了 meta 資料標記搜尋類型。

表 2. *Meta* 資料標記搜尋

meta 資料標記搜尋類型	格式	範例
標準	`MetadataTag:<value>`	`ApplicationProtocol:http`
萬用字元	`MetadataTag:*`	`CreditCardNumber:*`
範圍	`MetadataTag:[<start value> TO <end value>`	`Duration:[30 TO 56]`

相關概念:

第 21 頁的『文件註釋』
調查者可以對文件加上書籤，並新增附註至文件，以追蹤與其案例中的文件相關的構想。

布林組合

可以使用簡式布林運算子將多個查詢術語結合，以建立高度定向的查詢字串。 若經過適當組合，這些查詢字串可以返回完全符合調查者尋找內容的結果。

基本布林運算子為 AND、OR、NOT 與 ()。 AND 運算子指定兩個查詢術語在文件中都必須符合。 OR 運算子指定可在文件中找到任一查詢術語。 NOT 運算子使查詢術語無效，或移除符合無效查詢術語的結果。 () 運算子將查詢術語與值分組，以將函數套用至集合、套用多個值至單一函數，或澄清語法。

布林運算子必須大寫。

下表列出了布林運算子及查詢字串的範例。

表 3. 查詢字串的布林運算子

布林運算子	查詢字串範例	範例說明
AND	`TcpPort:80 AND Protocol:http`	使用兩個查詢術語來尋找所有標準 Web 資料流量。 如果在 8080 埠執行 Web 測試，則不符，因為兩個查詢術語並非皆為 true。
OR	`Collection:yahoo* OR Collection:cnn* OR Collection:msn*`	使用三個查詢術語將結果限制為來自 forensics 儲存庫中的 Yahoo、CNN 及 MSN 文件集合的結果。
NOT	`ApplicationProtocol:http AND NOT ServerTcpPort:(80 OR 8080 OR 81)`	搜尋使用非標準埠的資料流量。 第一個查詢術語尋找標準 HTTP 資料流量，而第二個查詢術語刪除使用可接受 HTTP 埠的所有資料流量。

()	`(ApplicationProtocol:http AND NOT ServerTcpPort:(80 OR 8080)) OR (ApplicationProtocol:pop* AND NOT ServerTcpPort:110)`
	
	`NOT (Collection:yahoo* OR Collection:cnn* OR Collection:msn*)`
		這些查詢有效使用括弧達到複式目標。若不使用括弧，則這些查詢將會更長，且公式化及除錯會更複雜。

查詢建置器工具

使用查詢建置器工具來建立搜尋或管理已儲存的搜尋。

查詢建置器工具以圖形方式向調查者顯示使用分類查詢術語清單建立強大搜尋的過程及範例。

表 4. 查詢建置器工具的參數

參數	說明
選取種類	過濾**選取欄位**清單中提供的 meta 資料標記清單。
選取欄位	用於標記 forensics 儲存庫中資訊的 meta 資料標記。
查詢範例	執行**查詢輸入**欄位中的查詢，並報告結果數。
新建	當您按**插入查詢**時，使用新建查詢來取代現有查詢。
AND	當您按**插入查詢**時，將新建查詢與現有查詢結合。 文件必須同時符合倆個查詢術語。
OR	當您按**插入查詢**時，將新建查詢與現有查詢結合。 文件必須符合其中一個術語。

調查者可以將搜尋儲存在檔案系統上的資料夾中，並進行整理，以容許在調查者之間共用。 調查者使用已儲存查詢的說明或名稱來作為參照、管理及瞭解用途。

查詢標籤上的**使用查詢**功能用於將儲存的查詢傳送至**搜尋準則輸入**欄位，以便執行。

調查者使用前一個查詢清單來尋找之前執行的查詢，然後選取要執行的查詢並按**插入查詢**來重新執行。

查詢過濾工具

查詢過濾工具使用作用中資料來提供視覺化提示，用於建置持續性過濾器。

查詢過濾器是持續性背景過濾器，可減少查詢字串詢問的作用中文件集。 透過使用過濾器，您可以減少可用文件集，而無需超載使用靜態查詢術語的查詢字串。 因此，您可以具有對查詢字串的更多控制。

查詢過濾器是開始調查的良好起點，因為它有依賴案例的過濾器類型清單、動態更新及即時結果摘要。 過濾器類型清單中會移入在您可用的案例中發現的所有值。 您可以快速查看您擁有之案例內包含的資料。 自動選取或清除過濾器類型清單項目，以更新結果摘要。 您可以在使用過濾器時，快速查看過濾器的有效性，以及文件集保留的大小。

針對您要重複使用的查詢，不建議調整預設查詢過濾器。 對於要保留的查詢，建立新的查詢過濾器。 如果您修改預設查詢過濾器，請在完成時將其重設，以避免將文件從後續搜尋查詢內錯誤地排除。

作用中的過濾器結果

調查者可在查詢過濾器工具的結果匯總區段內檢視作用中過濾器的結果。

變更過濾器時，摘要更新顯示文件總數，以及可用的文件計數。 文件總數為套用過濾器之前調查者可用的文件計數。 可用文件計數為套用過濾器之後可用的文件計數。 調查者使用這些計數來判斷其過濾器的有效性，並在建置時適當進行調整。

查詢過濾工具的搜尋過濾器

調查者過濾其指定狀況的資料。資料依過濾器類型分隔為群組，例如，IP 位址或 MAC 位址。

調查者可以使用邏輯動作開關，包含或排除清單中選取的項目。

每一個搜尋過濾器群組皆有一個邏輯動作開關，可以設定為包含或排除清單中選取的項目。 若設定為包含，則將清單中的項目與邏輯 AND 結合，表示每一個可用的文件皆包含選取的所有項目。 若設定為排除，則使用邏輯 OR，表示每一個可用的文件不包含選取的任何項目。

調查者可以使用 **UserQuery** 群組來公式化他們自己要新增至過濾器的查詢字串。

限制搜尋中的傳回文件數

您可以將過濾器新增至 IBM Security QRadar Incident Forensics 查詢，以限制在搜尋結果頁面中顯示的文件數或類型。

程序

1. 在 **Forensics** 標籤上，按一下**查詢過濾器**圖示。

   資料會依過濾器類型分隔為群組。
2. 在「搜尋過濾器」視窗中，為每種過濾器類型選擇是否將文件包含在搜尋結果，方法是按一下**包含**或**排除**。
3. 若要在過濾器群組中尋找項目，請遵循下列步驟：

a. 在**過濾器類型**欄中，展開過濾器群組。
b. 在「搜尋」視窗中，選取準則，然後按一下**尋找**。

當您在 **Webcategory** 過濾器群組中搜尋記錄時，畫面上會顯示所有相符的種類欄位。例如，當您搜尋 **Webcategory equal chat** 時，畫面上會顯示**會談** 及相關的種類，如**即時傳訊**、**Webmail/統一傳訊**、**搜尋引擎/Web 型錄/入口網站**及**雲端**。

文件註釋

調查者可以對文件加上書籤，並新增附註至文件，以追蹤與其案例中的文件相關的構想。

可以在主要結果畫面上為文件加上書籤，也可以在 surveyor 工具中的依時間順序網格上進行，該網格顯示互動期間交換的文件順序。 由於查詢與調查可能較為複雜，調查者可以為所有記錄加上書籤，包括不是非常感興趣的文件。 使用書籤則不需要重建複式查詢及調查範圍。為記錄加上書籤之後，可以建立註釋。

在調查期間，有時需要追蹤兩條或多條路徑。 使用瀏覽器功能複製您在處理的現行標籤。 複製標籤可以協助您避免在追蹤其他路徑時必須記住返回位置，或是記住如何進入分支點。 您可以根據需要，任意次數地複製現行標籤。 追蹤不同標籤內的每一個不同路徑，以及整個過程中的書籤相關文件。 您可以新增附註，指定導向每一個加註書籤之文件的路徑。

附註是在調查時記錄想法的方式。 附註只能由管理者移除。 以調查者的使用者 ID，以及輸入時的時間戳記標記附註。 當匯出文件時，附註與重新建構的文件及其屬性一併輸出。

相關概念:

第 18 頁的『Meta 資料標記』
一般實體標記為容許調查者從相關文件快速擷取確切的結果集。

第 4 章 調查工具

調查者使用 Surveyor、Digital Impressions、Export 與 Visualize 工具，以不同方式管理資料。

搜尋結果頁面是 **Forensics** 標籤上的預設頁面。搜尋結果可在**網格**標籤上獲得。調查者使用網格上的搜尋結果，快速搜尋及存取文件。 在**網格**標籤上，使用 Surveyor、Digital Impressions、Export 與 Visualize 工具來進一步調查。

列指示器

列指示器可為結果集中返回的每一個文件提供唯一的 ID。 使用列指示器將文件及所有必需的相關文件傳送至「重新建構視圖」視覺化工具。

列排序

您可以對網格中顯示的列進行排序。 因為結果總數可能大於網格上顯示的結果數，所以無法排序整個結果集。

文件已檢視指示器

文件已檢視指示器是一個在紅色與綠色之間切換的小圓圈，用於指示調查者已檢視此文件。

文件選擇

調查者使用顯示的文件選擇器來選擇結果網格中顯示的文件數。 您可以使用 SELECT ALL 來傳送文件給後續函數，且可以傳送大量文件進行處理或視覺化。 當您使用所顯示文件選取器選取文件時，將會選取所有文件，而不僅是網格內呈現的文件。

網路與文件視覺化

調查者使用視覺化工具來偵測型樣、瞭解指定時段內網路資料流量及文件壅塞最多的位置，並檢視可疑內容。 例如，調查者可以視覺化網路資料流量的型樣，如辦公時間之後存取的伺服器。

VGrid 工具劃分為時間區塊。 在網格上，可疑內容（例如，網路資料流量或文件）由紅色矩形表述。 綠色矩形表示一般內容。 鮮明的顏色區塊指示資料流量較多。 顏色飽和度越高，資料流量越大。 時間區塊的明亮度與 VGrid 工具中顯示的現行資料相關。例如，當不同的時間區塊載入更多資料時，明亮的彩色時間區塊變得更暗。

調查者可以檢視網路資料流量的類型，以及每一個時間區塊內包含內容的文件數。

檢查時間區塊內的網路資料流量及文件

調查者可能想要檢查特定時間區塊內的個別文件、瀏覽的網站，或傳送的電子郵件。

程序

1. 在 **Forensics** 標籤上，選取 **VGrid** 標籤。
2. 使用下列其中一個選項來檢查時間區塊內的內容：
   - 若要檢視網路資料流量的類型及文件數量，請移至時間區塊。
   - 若要搜尋時間區塊內的內容，請選取一或多個時間區塊。 按一下滑鼠右鍵選取**搜尋選取的時間區塊**。
   - 若要檢視事件的順序，請選取時間區塊，然後選取 **Surveyor**。
   - 若要視覺化內容，請選取時間區塊，然後選取**視覺化**。

Surveyor 工具

使用 Surveyor 工具可視覺化安全事件中發生事件的順序。

調查者使用此工具來查看可疑的攻擊者所檢視的內容，及其動作。 Surveyor 工具以類似影片的視覺化程式描述了安全事件中活動的時間順序。 由於 Surveyor 是面向時間的，從結果畫面選擇單一文件不會顯示很多內容。 如果選取的文件太少，請展開**屬性**標籤中所選取文件周圍的時間半徑。 按一下**顯示環境定義**鏈結來展開時間。

使用**屬性**標籤可顯示憑證資訊和 meta 資料。用滑鼠右鍵按一下 IP 位址或埠，以根據事件、流程和資產來進行過濾，或者用滑鼠右鍵按一下 MAC 位址，以根據事件和資產進行過濾。

您可以依案例時間、通訊協定及 IP 位址過濾查詢。

您可以使用**清單**標籤，以查看已傳送及接收之文件的時間順序清單。

綠色文件 ID 數指示調查者已檢查文件，而含有紅色 ID 數的文件則未被檢查。

重新建構文件視圖

視圖標籤顯示在「清單」視圖中的左側畫面上所選之文件的重新建構視圖。

這個左側排序與右側重新建構的強大組合能夠提供查看可疑攻擊者在網路上的所見及動作。 除了遍訪網路的可見文件以外，Surveyor 還可顯示背景中電腦之間的信號交換，及發生的憑證交換。

相關工作:

第 33 頁的第 5 章, 『調查 IP 位址的網路資料流量』
若要視覺化安全事件期間發生的對話中的相關內容，您可以回復並重新建構與 IP 位址相關聯的網路資料流量。 您也可以在與 IP 位址相關的現有案例中搜尋。

擷取的文件內容

文字標籤顯示從文件擷取的內容。 文件內容未格式化。

此文字來自搜尋引擎檢索程式。

QRadar Incident Forensics 中的文件匯出

在 IBM Security QRadar Incident Forensics 中，所有匯出的文件（除匯出的 pcap 文件以外），包含重新建構的文件、文件的原始文字、屬性及附加至文件的注意事項。

pcap 文件匯出時，不會進行重新建構。例如，當您匯出網頁時，會下載瀏覽器在主要連線期間下載的任何項目。通常，在主要連線期間下載大部分文字內容。但是，當今大部分瀏覽器使用多個連線下載更多項目（如樣式表及影像），這不是匯出的一部分。當您匯出時，不會先重新建構 pcap 內容。

其他範例是複式通訊協定（如 FTP 及 VOIP），其中具有主要指令及控制連線與個別資料連線。如果您為 VOIP 呼叫或 FTP 下載匯出 pcap 檔案，則不會重新建構資料，且您可能會取得非預期的結果。

將文件匯出為 pcap 檔案

您可以從多個 IBM Security QRadar Incident Forensics and IBM Security QRadar Packet Capture 軟體驅動裝置將文件匯出為 pcap 檔案。

限制：您匯出為 pcap 格式的內容無法重新建構。

程序

1. 要匯出選定文件中的資料，請在 **Forensics** 標籤的回復網格中，選取文件旁邊的勾選框，然後按一下**匯出**。

   您最多可以選取 25 文件來匯出為 pcap 格式。
2. 從**選取匯出類型**清單中，按一下 **PCAP**。
3. 匯出 QRadar Incident Forensics 主機的所有文件之後，您可以按一下**下載**。
4. 如果匯出文件失敗，請按一下**失敗**訊息再次匯出文件。

結果

如果您匯出單個 pcap 檔案，則會下載該檔案。如果您匯出多個 pcap 檔案，則會將這些 pcap 檔案組合到一個壓縮檔 (.zip) 中並下載該壓縮檔。

每一個文件都儲存文件最初源自的 QRadar Incident Forensics 主機的IP 位址及 QRadar Packet Capture 裝置的 IP 位址。如果您移除 QRadar Incident Forensics 主機或移動 QRadar Packet Capture，則您可能無法匯出。

Digital Impression

數位印象是一組可識別身分軌跡的關聯和關聯編譯集。 Digital Impression 會重新建構網路關係，以協助顯示攻擊實體的身分、其通訊方式及其通訊內容。

使用 Digital Impression 工具，可以快速回答下列重要問題：

- 此可疑攻擊者、電腦或 IP 位址的哪些狀況已知？
- 此可疑攻擊者曾與誰對話？
- 其聯絡人網路中的對象？
- 可疑攻擊者是否嘗試隱瞞其身分？

線上 ID

線上 ID，如電子郵件位址、Skype 位址、MAC 位址、聊天 ID、社交媒體 ID，或 Twitter ID 可用來識別實體或人員。 於網路及文件中發現的已知實體或人員將會自動貼上標籤。

IBM Security QRadar Incident Forensics 將彼此互動的標籤 ID 關聯起來，產生數位印象。

數位印象報告中的集合關係代表所收集的與攻擊者、網路相關實體或任何數位印象 meta 資料項目關聯的電子顯示狀態。 調查者可以按一下與文件關聯的任何標籤數位印象 ID。 產生的數位印象報告以表格格式列出，依 ID 類型整理。

取得關係資訊

數位印象報告顯示中心 *ID* 與其他所有 ID 之間的互動。 中心 *ID* 是安全事件中感興趣來源的線上 ID。

許多種類中最上層 ID 一般為該 ID 類型或種類中的中心 ID 身分。 例如，如果 ID 為 MAC 位址，則具有大部分互動的電子郵件位址可能屬於擁有該電腦的可疑攻擊者。但是，如果動態指定 IP 位址，則您還必須調查某個時間範圍內指定的 IP 位址。

其他種類與中心 ID 之間的關聯一般沒有這麼強。 在您決定根據 Digital Impression 採取動作之前，請驗證獨立來源的資料。 使用 Digital Impression 擴大調查半徑，以取得更多可疑的攻擊者以及實體。

調查關係以追蹤身分軌跡

Digital Impression 可重新建構網路關係，以協助您確定攻擊實體及與其通訊之其他實體。

Digital Impression 工具顯示相關事件的頻率配送。 工具顯示實體之間的關係，並計數關係。 計數越高，關係越強。 例如，如果您檢視電子郵件位址與其他實體之間的關係，則可以查看誰與誰進行通訊。 您可以檢視與電子郵件位址相關聯的 IP 位址、可疑者造訪的 IP 位址及與電子郵件位址相關聯的其他名稱。

在分佈式部署中，您可以選擇查看組織內某個節點的關係。

程序

1. 從回復網格中的文件清單選取一個結果，然後按一下 **Digital Impression** 標籤。
2. 從清單中選取要探索的項目。

   依預設，Digital Impression 報告以表格格式列出，依 ID 類型整理。 顯示與中心 ID 互動的所有 ID。互動 ID 依 ID 類型整理，依互動頻率排序。
3. 如果您看到感興趣的 ID，請選取它。

   ID 為超鏈結，您可以用它們作為其他報告的中心 ID。此時會建立另一個標籤，並顯示新的中心 ID。 您可以查看與指定之可疑攻擊者互動的對象，然後查看可疑的互動對象。 您可以將調查半徑擴大至更多可疑的攻擊者，以及與其互動的實體。
4. 若要查看另一部主機，請從**選取遠端主機**清單選取 IP 位址。

   在分佈式安裝中，您可以選擇 QRadar Incident Forensics 主機，然後檢視 digital impression。 預設視圖為主要主機，但您可以選取與 QRadar Incident Forensics 主機關聯的任何次要主機。
5. 若要查看中心 ID 與其他 ID 互動之關聯與關係的視覺化，請按一下**視覺化資料**標籤。

視覺化工具

您可以視覺化探索多個屬性及資料種類內的關聯與關係。

使用「視覺化」視窗來查看一個、兩個或大量所選文件的 meta 資料關聯圖。當使用大量所選文件時，調查者會得到一個 meta 資料關係及相關頻率的綜合性視圖。 然後，調查者可以追蹤這些路徑，進一步調查調查事件。

透過變更一個關係或全部關係，可使用不同關係輕鬆重建所選文件的視覺化。

視覺化顯示所選文件中包含的每一種關係，並顯示關係的頻率。 每一個節點表示與所選文件相關的每一個不同的 meta 資料。 大小傳送與其他節點比較的相對頻率。 鏈結顯示在不同 meta 資料部分之間發現的連線，並透過大小傳送頻率。 調查者可以使用節點來識別可能的通路，以便進一步調查。

視覺化關係及關聯

使用「視覺化」視窗來查看回復文件屬性之間的關係。例如，您可以檢查與特定電子郵件位址通訊的電子郵件位址。

程序

1. 在回復網格中，按一下您要調查之文件的勾選框，然後按一下**視覺化**。
2. 選取佈置、要顯示的文件數，以及要查看之屬性之間的關係，然後按一下重新整理。
3. 使用縮放控制項來查看更多或更少的映像檔明細。
4. 若要執行新搜尋或修改作用中的過濾器，請用滑鼠右鍵按一下節點。

   從環境定義相關功能表，可以將這部分 meta 資料帶回，以執行新搜尋。 您還可以修改作用中的過濾器，以包含或排除 meta 資料。

   限制：在一個「視覺化」視窗中，您一次最多可以檢視 9999 個文件。

可疑或惡意內容的構件分析

作為安全分析師，您可以透過分析重新建構的構件（檔案和影像）來查看迴避偵測的威脅。若要瞭解合作程式及構件之間的關聯，您也可以調查這些檔案及影像的鏈結。

範例 - 使用構件分析來尋找攻擊來源（病患零）

John 是 Replay Industries 的安全分析師。儘管施實了所有安全措施，仍有數個系統受到感染病毒。確定及隔離這些系統之後，John 需要找出這些系統受到病毒感染的原因，以及是否存在類似的其他資產受損。

從 IP 位址進行封包回復

從 IP 位址開始加上涉及的大致時間範圍，John 能夠使用 QRadar Incident Forensics 來回復相關的封包資料。

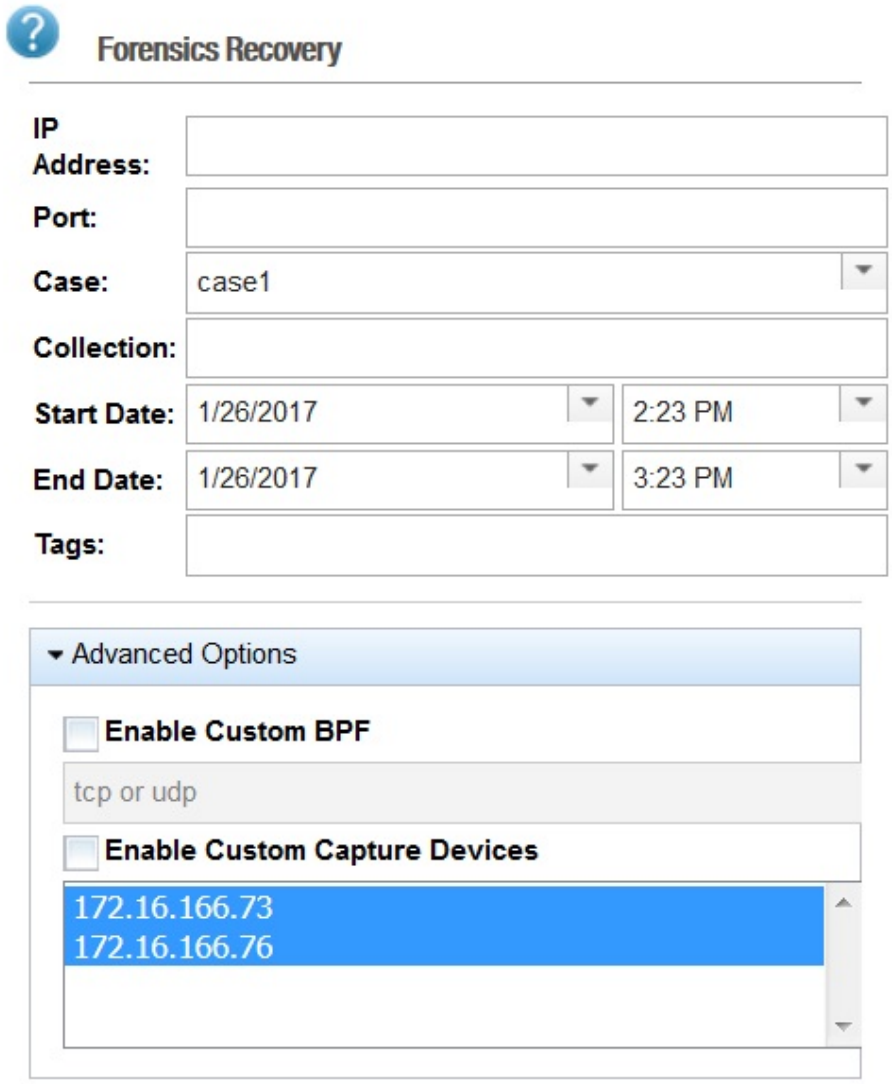


圖 *1.* 從 *IP* 位址回復

檔案分析

John 使用 QRadar Incident Forensics 內所含的檔案分析功能開始，尋找執行檔內容。現在，他可以看到所有檔案清單、傳送頻率、它們是否包含內嵌檔或 Script，及其熵分數。John 可以快速看到 QRadar Incident Forensics 標示為可疑內容和包含內嵌 Script 的影像檔。

Doc #	File Name	Extension	Description	Protocol	Frequency	Suspect Content	Embedded Script	Embedded Files	File Size (Bytes)	File Hash (SHA-256)	Entropy
1	index.php	php	CSS File	http	1	No Suspect Content	No Embedded Script	0	1916	70c6e673cd0150b1ffa89e	4.93731
2	index.php	php	CSS File	http	1	No Suspect Content	No Embedded Script	0	163060	dbbb35dcf2e494f068b9d1	5.74523
3	index.php	php	JavaScript	http	1	No Suspect Content	No Embedded Script	0	164112	909a0b9fa48182b58dd85	5.38451

圖 *2.* 檔案分析屬性

檔案熵評分可測量資料的隨機性，並用於尋找已加密的惡意軟體，而熵分佈亦能明確顯示不屬於檔案的部分。進一步分析證明該檔案包含新格式的惡意軟體，因此迴避了現有安全手段的偵測，造成了系統受到病毒感染。

在下圖中，熵被用作每個位元組的位元變化性指示器。因為資料單元中的每一個字元都由一個位元組組成，所以熵值指示字元的變體，以及資料單元的壓縮能力。檔案中的熵值的變化可能指示檔案中隱藏可疑的內容。例如，熵值高可能指示資料已加密並壓縮儲存，熵值低則可能指示在執行時期，於不同區段中解密和儲存內容。

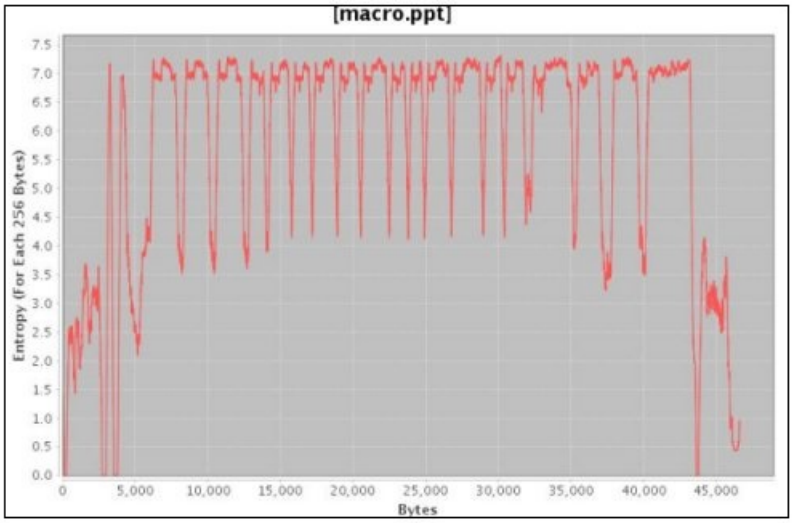


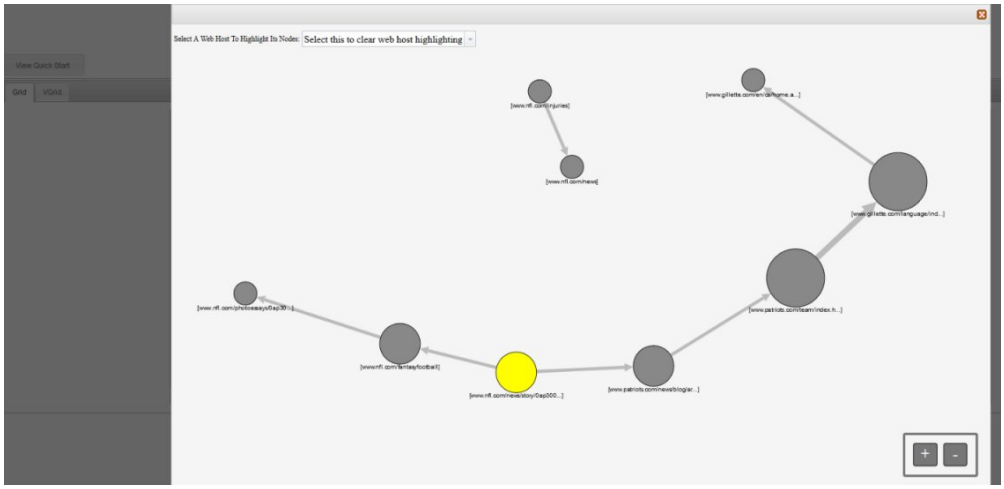
圖 *3.* 顯示內嵌 *Script* 的檔案熵圖的範例

John 現在需要瞭解該檔案來自何處，以及還有哪些人可能有此檔案。John 使用 QRadar Incident Forensics 來快速尋找提供受感染影像檔的 Web 伺服器。有問題的網頁常用於播送大家最愛的 NFL 團隊的最新新聞，並已受損。即便網站包含許多影像，但 John 使用檔案分析只發現一個影像包含內嵌惡意軟體。

視覺化網站通訊的鏈結分析

為了判定其他可能受影響的系統，John 使用鏈結分析來快速查看檢視的所有網站，但將與 Replay 有生意來往的公司網站流經的大量資料流量除外，受感染的主機仍然能夠明確看到一小部分存取。John 分析這些鏈結以查看其網路上是否還有其他伺服器用於存取此 Web 主機。

在 John 的調查中，他使用圖形中的節點（代表網頁）和箭頭（代表網頁之間的關係或交易）來快速評量資料流量的型樣，並查看文件的遍訪方式。節點越大，文件路徑中包含的鏈結越多，鏈結箭頭越大，鏈結的使用次數越多。



作為受歡迎的 NFL 新聞網站，會看到大量其他伺服器與該 Web 主機交互，並造成可能的影響並非意外。

影像分析

為了縮小範圍至哪些伺服器下載了惡意影像檔，John 切換至影像分析並且可以快速查看已傳送或接收的所有影像檔。

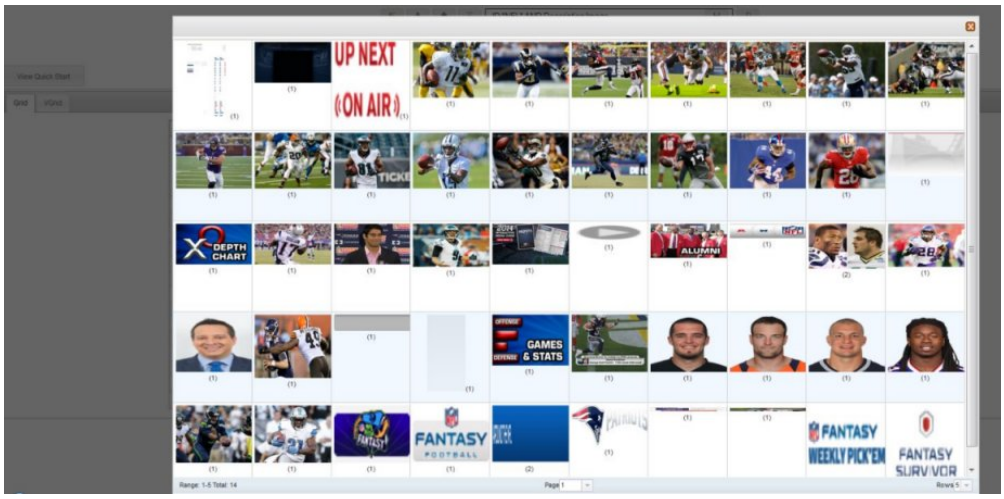


圖 4. 影像分析和影像配送的範例

John 快速確認了所有受感染的伺服器及 2 部未注意到的伺服器均存取受損的影像檔。

John 還確定了其他數個存取相同網站的伺服器未下載受感染的檔案。現在，John 已取得隔離這兩部額外伺服器所需的資訊，並為受感染的檔案新建一個檔案雜湊，以便 Replay Industries 能夠上傳並與 IBM X-Force® Exchange 上的其他人共用。

分析內嵌內容及惡意活動的檔案

若要調查檔案以瞭解隱藏的威脅，您可以查看檔案的熵值、下載內嵌檔和 Script，以進行進一步分析，並檢視文件及其屬性。

因為侵入者可以使儲存器檔案內二進位檔的內容變模糊，所以您可以使用 IBM Security QRadar Incident Forensics 中的檔案分析來檢查檔案是否包含內嵌的 Script 或其他二進位內容。

檔案熵可測量檔案中資料的隨機性，並用於確定檔案是否包含隱藏資料或可疑的 Script。隨機性的尺度由 0（非隨機）至 8（完全隨機），如加密檔案。單元壓縮程度越高，熵值越低；單元壓縮程度越低，熵值越高。

在下圖中，熵被用作每個位元組的位元變化性指示器。因為資料單元中的每一個字元都由一個位元組組成，所以熵值指示字元的變體，以及資料單元的壓縮能力。檔案中的熵值的變化可能指示檔案中隱藏可疑的內容。例如，熵值高可能指示資料已加密並壓縮儲存，熵值低則可能指示在執行時期，於不同區段中解密和儲存內容。

程序

1. 在 **Forensics** 標籤上，從**網格**視圖選取一或多個回復的檔案。
2. 從網格頂端的調查工具功能表中，按一下**檔案分析**。

   在結果中，網格的每一列包含文件的一項分析資料，例如：檔名、說明、是否偵測到可疑內容及熵值。
3. 若要依特定屬性來排序檔案（如熵），按一下關聯的直欄標題。
4. 從檔案清單中，用滑鼠右鍵按一下檔案，以進行進一步調查。
   - 若要檢查文件及其屬性，按一下**顯示文件**。
   - 若要檢查熵圖，並查看內嵌的檔案或 Script 是否包含惡意軟體，按一下**顯示熵**。

     您可以使用熵值作為檔案是否包含惡意內容的指示。例如，ASCII 文字檔一般都是高度壓縮的，且具有較低的熵值。加密資料一般無法壓縮，且總是具有較高的熵值。惡意軟體通常經過壓縮，並隱藏在檔案和圖像中。
   - 若要下載內嵌檔案，按一下**解壓縮內嵌檔案**，並選取要下載的檔案。

     此選項僅適用於含內嵌檔或 Script 的文件。檔案將會下載至您 Web 瀏覽器的下載位置。請注意，不要在未經保護的環境下打開可能有害的 Script。

分析影像中的隱藏威脅和可疑活動

檢視的影像依大小和相關性排序，並在括弧中顯示頻率數字。如果有員工使用公司資源查看不恰當、限制或禁止的影像時，此分析可能會有幫助。例如，影像可能與作為安全侵害目標的飛機、特定建築物或地點相關。

透過影像分析，您可以在一個畫面中檢視一或多個封包擷取檔案中一或多個文件的大部分相關影像，而不會強制開啟每一個文件並檢視影像。

程序

1. 在 **Forensics** 標籤上，從**網格**視圖中選取說明中包含影像的一或多個文件。
2. 從網格頂端的調查工具功能表中，按一下**影像分析**。

   在結果中，文件內所包含的所有影像的縮圖版本都以相關性順序顯示。影像旁邊括弧內的數字指示文件中影像的實例數。如果您將游標放在縮圖影像上，則影像會變大。
3. 用滑鼠右鍵按一下影像，以進行進一步調查

- 若要檢查影像及其屬性，按一下**顯示文件**。
- 若要檢查熵圖，並查看影像是否可能包含惡意軟體，按一下**顯示熵**。

  您可以使用熵值作為檔案是否包含惡意內容的指示。例如，點陣圖影像檔和 ASCII 文字檔一般都是高度壓縮的，且具有較低的熵值。加密資料一般無法壓縮，且總是具有較高的熵值。惡意軟體通常經過壓縮，並隱藏在檔案和圖像中。

連線和關係的分析鏈結

在鏈結分析中，鏈結顯示受檢視網站之間的共同性。在安全事件調查期間，您可以快速查看重疊的位置，以及人員之間的通訊方式。

例如，如果您認為有一組嫌犯在分工合作，但尚未確定其工作方式，則您可以查看多個使用者的文件集，並使用鏈結分析來顯示共用的網頁。然後，您可以調查特定網站。

程序

1. 在 **Forensics** 標籤上，從**網格**視圖選取一或多個網頁。
2. 從網格頂端的調查工具功能表中，按一下**鏈結分析**。

   如果網站之間存在關係，則 Cytoscape 圖表將網頁顯示為圓圈（節點），將網頁鏈結顯示為箭頭。節點越大，文件路徑中包含的鏈結越多，鏈結箭頭越大，鏈結的使用次數越多。所選取的節點為黃色。
3. 若要調查來自從特定 Web 主機的通訊，請從**選取 Web 主機**清單中選取 Web 主機。

   代表來自所選 Web 主機之網頁的節點以深灰色圓圈強調顯示。
4. 若要放大或縮小圓圈（節點）和箭頭的大小，請使用放大 (+) 或縮小 (-) 控制項。

   您也可以將滑鼠滾輪向上或向下捲動，以放大或縮小節點和箭頭的大小。
5. 若要移動一或多個節點，請按一下並拖曳節點。

   您可以點擊背景中的任何位置，以便移動整個圖形，然後按住並拖曳。

從文件的屬性頁面執行回復

當您檢視文件的**屬性**標籤時，您可以針對 IP 位址或埠執行回復。

程序

1. 從 **Forensics** 標籤上的「搜尋」頁面中，執行搜尋。
2. 從傳回的文件清單中，按一下其中一個文件將其開啟。
3. 按一下**屬性**標籤。
4. 按一下 IP 位址或埠。
5. 從功能表中，按一下**針對以下項目執行回復**。

第 5 章 調查 IP 位址的網路資料流量

若要視覺化安全事件期間發生的對話中的相關內容，您可以回復並重新建構與 IP 位址相關聯的網路資料流量。 您也可以在與 IP 位址相關的現有案例中搜尋。

當透過 IP 位址重新建構網路資料流量時，會建立事件。 調查者可以視覺化安全事件的事件順序，或檢視事件中的文件。

IBM Security QRadar Incident Forensics 可對每一個回復檔案中的所有可用網路資料、檔案資料、meta 資料及文字字元建立索引。

在分佈式部署中，多個擷取裝置及 QRadar Incident Forensics 主機會擷取並處理資料。您可以檢視聚集的事件回復結果，或依主機與擷取裝置排列的結果。

程序

1. 若要建立案例並從封包擷取裝置取得資料，請在 QRadar 中，用滑鼠右鍵按一下 IP 位址，然後選取**執行 Forensics 回復**，或者按一下 Forensics 回復圖示  。
   a. 使用下列資訊來設定 Forensics 回復參數：

表 *5. Forensics* 回復參數

參數	說明
IP 位址	使用指令來區隔多個 IP 位址。如果未輸入任何 IP 位址或埠，則使用預設的 TCP 或 UDP。
埠	使用逗點來區隔多個埠。
案例	案例名稱必須是唯一的。
集合	回復的資料分組至集合內，並與案例相關聯。 集合名稱必須是唯一的。 如果案例中已存在此集合名稱，則會刪除原始集合。
標記	選用項目。用於從相關文件快速擷取確切結果。 使用逗點來區隔多個標記。僅使用英數字元；不接受特殊字元。
啟用自訂 BPF（Berkeley 封包過濾器）	管理者可以使用。選取該勾選框以啟動 BPF 輸入欄位，您可以在其中指定 IP 位址與埠。
啟用自訂擷取裝置	管理者可以使用。選取該勾選框會在您的部署上產生 PCAP 裝置清單。選取一個或多個裝置，以僅查看來自那些裝置的資料流量。

   b. 按一下**確定**，然後按一下 Forensics 標籤。

      疑難排解：如果您看到一則訊息，說明您無權回復資料，請確保安全設定檔具有對 IP 位址的存取權。 在部分實例中，如果您在**標籤**欄位中使用 # 字元，則可能看到該訊息。

   c. 按一下事件圖示  以檢視您的事件。在階層中導覽時展開或收合內容。
   d. 若要檢視事件中的文件，請按一下**跳至搜尋頁面結果**。
   e. 若要視覺化事件的事件順序，請按一下**跳至 Surveyor 頁面結果**。

f. 若要移除或取消特定事件，按一下**刪除或取消此事件**。

g. 若要重新執行前一個 Forensics 回復工作，請按一下**重新執行此 Forensics 回復**。例如，如果結果返回不完整的資料，請重新執行 Forensics 回復來包含不同的 IP 位址，或變更前一個執行回復工作中指定的時間範圍。

2. 若要搜尋 QRadar 中的現有案例，用滑鼠右鍵按一下 IP 位址，然後按一下**執行 Forensics 搜尋**。

a. 在 **Forensics** 標籤上，按一下事件圖示。

b. 若要調查與事件相關聯的活動聚集，可將滑鼠移至案例以強調顯示，然後按一下搜尋圖示。

c. 若要調查分佈式部署中依 QRadar Incident Forensics 主機與擷取裝置排列的活動，請展開**案例**項目，然後展開**集合**項目。

d. 若要檢視事件中依時間順序排列的互動清單，請將滑鼠移至集合以強調顯示，然後按一下 Surveyor 圖示。

相關概念:

第 24 頁的『重新建構文件視圖』

視圖標籤顯示在「清單」視圖中的左側畫面上所選之文件的重新建構視圖。

自訂 BPF

若要在執行自訂 Forensics 回復時僅查看部分類型的資料流量，您可以選擇建立自訂「Berkeley 封包過濾器 (BPF)」。

在「Forensics 回復」上，選取勾選框以啟動 BPF 輸入欄位，您可以在其中指定 BPF 過濾器來過濾網路資料流量。

使用 BPF 語法來指定 BPF 過濾器。 表示式由一或多個基本元素組成。 基本元素是對網路通訊協定標頭中一或多個欄位的參照。例如，主機、埠、TCP 埠都是基本元素。您可以使用 AND、OR 和 NOT 運算子來建置複式過濾表示式。

下面是過濾器的範例：

```
host 10.0.0.1
port 80
tcp port 80 and host 10.0.0.1
host 10.0.0.1 or host 10.0.0.2 or port 80 or port 443
```

若要建立 BPF，您必須有權存取管理者使用者角色。所有非管理者使用者都具有 BPF 文字欄位的唯讀存取權。管理者使用者可以輸入任何 BPF 表示式。

限制：Forensics 回復將套用提供的 BPF。如果您的回復結果非預期，請檢查回復輸入和 BPF 以確保準則是否正確。

即便當自訂 BPF 未在使用時，BPF 欄位也總是包含 **IP 位址**或**埠**欄位的內容。如果未輸入任何 IP 位址或埠，則自訂 BPF 使用預設的 TCP 或 UDP。

聲明

本資訊係針對 IBM 在美國所提供之產品與服務所開發。

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

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

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

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

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

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。

4544本資訊中任何對非 IBM 網站的敘述僅供參考，IBM 對該網站並不提供保證。這些網站上的內容並非本 IBM 產品內容的一部分，貴客戶使用這些網站時應自行承擔風險。

IBM 得以各種 IBM 認為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為了 (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 Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785US

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。

執行效能資料和引用的客戶範例僅供說明之用。實際效能結果可能依特定的配置和作業條件而改變。

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

有關 IBM 未來方向或意圖的陳述僅代表其目標，如有變更或撤銷並不會另行通知。

所有 IBM 價格為 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。 為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，如與實際人名或企業有任何類似之處，純屬巧合。

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，網址為 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。

產品說明文件的條款

這些出版品的使用許可權係遵循下列條款而授予。

適用範圍

下列條款係 IBM 網站使用條款之特別條款。

個人使用

貴客戶可以為了非商務性的私人用途而複製這些出版品，但必須保留所有專利注意事項。未經 IBM 明示同意， 貴客戶不得散佈、顯示或製作這些出版品或其任何部分的衍生著作。

商業使用

貴客戶可以在企業內複製、散布和顯示這些出版品，但必須保留所有專利注意事項。未經 IBM 明示同意，貴客戶不得製作這些出版品的衍生著作，也不得於企業外重製、散佈或顯示這些出版品或其任何部分。

權利

除了本項許可權所明確授予者之外，並未明示或暗示授予出版品或任何資訊、資料、軟體或其中的其他智慧財產的任何其他許可權、授權或權利。

若 IBM 審慎評估後認為本出版品用途已危及其利益，或 IBM 認為上述指示未被適當遵循，IBM 保留隨時撤銷此許可聲明的權利。

除非完全符合所有適當的法律和規章，其中包括所有美國輸出法律和規章，否則，貴客戶不能下載、輸出或再輸出本項資訊。

IBM 不提供這些出版品內容的任何保證。這些出版品只依「現狀」提供，不含任何明示或暗示的保證，其中包括且不限於可售性或符合特定效用的暗示保證。

IBM 線上隱私權聲明

IBM 軟體產品（包括作為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為了其他目的。 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啟用的功能。

如果為此「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（網址為 http://www.ibm.com/privacy ），以及 IBM 的線上隱私權條款（網址為 http://www.ibm.com/privacy/details），以及「IBM 軟體產品及軟體作為服務隱私權條款」（網址為 http://www.ibm.com/software/info/product-privacy）。

名詞解釋

本名詞解釋提供 IBM Security QRadar Incident Forensics 軟體及產品的術語及定義。

本名詞解釋中使用下列交互參照：

- 請參閱將您從非偏好的術語引導至偏好的術語，或者從縮寫引導至完整形式。
- 另請參閱將您引導至相關或對照術語。

如需其他術語及定義，請參閱 IBM Terminology 網站（在新視窗中開啟）。

『三劃』 『五劃』 『六劃』 『七劃』 『八劃』 『九劃』 第 40 頁的『十劃』 第 40 頁的『十一劃』 第 40 頁的『十二劃』 第 40 頁的『十三劃』 第 40 頁的『十四劃』 第 40 頁的『十八劃』 第 40 頁的『D』 第 40 頁的『M』 第 40 頁的『S』

三劃

已吸收網路資料流量 (ingested network traffic)
這是取證取消防護處理程序已處理的已擷取網路資料流量。

五劃

布林運算子 (Boolean operator)
這是在評估作業集時指定邏輯運算 AND、OR 或 NOT 的內建函數。布林運算子為 &&、|| 及 !。

加密 (encryption)
在電腦安全中，該處理程序會將資料轉換為難理解的形式，以便無法取得原始資料，或者只能透過使用解密處理程序取得。

六劃

回復工作 (recovery job)
這是回復所查詢擷取資料並將它轉遞至取消防護裝置以供吸收的處理程序。

交談 (conversation)
兩個以上網路端點之間取證重新建構的資料流。例如，社交網路交談。

安全發生事件 (security incident)
這是一般網路作業違規、已受損或受攻擊的事件。

收集 (collection)
這是與案例相關聯的特殊命名的資料集。例如，依序的已擷取網路封包集。

七劃

攻擊 (attack)
這是未獲授權人員損壞軟體程式或網路系統作業的任何嘗試。另請參閱攻擊者 (attacker)。

攻擊 (offense)
為回應受監視條件而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。

攻擊者 (attacker)
這是嘗試對資訊系統造成危害或存取未用於一般存取之資訊的使用者（人員或電腦程式）。另請參閱攻擊 (attack)。

身分 (identity)
資料來源中的屬性集合，代表人員、組織、地點或項目。

八劃

取消防護 (decapping)
這是解除編譯封包擷取資料以便產生所有所吸收資料作為結果報告而使用的處理程序。

取證檢查者 (forensic investigator)
這是從取證儲存庫中的網路資料流量與文件擷取相關資料的使用者。

九劃

封包擷取軟體驅動裝置 (packet capture appliance)
這是截取並記載資料流量資料的獨立式軟體驅動裝置。

封包擷取資訊 (packet capture information)
這是擷取裝置收集的資料流量資料資訊。

軌跡 (trail)
這是將案例中設計個人連接至案例外部個人的 Digital Impression。

十劃

連續收集電子顯示狀態 (continuously collected electronic presence)
這是作為所鏈結 Digital Impression 集合的攻擊者線上身分。

流程記錄 (flow record)
這是兩個主機之間的交談記錄。

案例 (case)
這是資料庫內包含之與特定調查相關的資訊。

通訊協定檢查程式 (protocol inspector)
這是設計以從網路通訊協定（例如 HTTP 或 FTP）擷取取證資料的特殊化檢查程式。

十一劃

異常 (anomaly)
與預期網路行為的偏差。

猜想 (hypothesis)
這是根據案例中收集之可用證據的所提出發生事件說明。猜想必須可測試且可檢驗。

十二劃

超流程 (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。

發生事件 (incident)
請參閱安全發生事件 (security incident)。

十三劃

置中 ID (centering identifier)
這是所有其他 ID 都已與其進行互動的種類項目。置中 ID 是調查中的中央項目。

資料流量 (traffic)
這是資料通訊中，傳輸以通過路徑中特定點的資料數量。

十四劃

種類 (category)
這是根據特定說明或分類分組的項目集。種類可以是維度內不同的資訊層次。

漏洞 (vulnerability)
作業系統、系統軟體或應用軟體元件中的安全漏洞。

網域檢查程式 (domain inspector)
這是設計以從特定網域網站解除建構並擷取取證資料的特殊化檢查程式。

十八劃

擷取裝置 (capture device)
請參閱封包擷取軟體驅動裝置 (packet capture appliance)。

瀏覽途徑 (breadcrumb)
這是顯示網站內使用者位置的 Web 介面元素。它通常是在頁面頂端或底端顯示的一系列超鏈結。這些鏈結指出已檢視頁面，且可讓使用者導覽回起始位置。

D

Digital Impression 關係 (digital impression relationship)
這是與案例相關之標籤 ID 之間的關係。

Digital Impression
這是包含個別案例內彼此相關之標籤 ID 的報告。

M

meta 資料 (metadata)
這是說明資料性質的資料；敘述性資料。

meta 資料關聯圖 (metadata relational map)
這是顯示案例文件相關 meta 資料的圖。

S

Surveyor 工具 (surveyor tool)
這是顯示視覺化程式中安全發生事件內依時間順序活動的工具。

索引

索引順序以中文字，英文字，及特殊符號之次序排列。

〔六劃〕

〔九劃〕

〔十劃〕

〔十二劃〕

〔十三劃〕

〔十七劃〕

D

I

M

Printed in Taiwan