使用Umbrella檢視或爭議IPS誤報

目錄

簡介

本文說明如何使用Cisco Umbrella檢查或爭議入侵防禦服務(IPS)誤報。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據Cisco Umbrella。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

概觀

Cisco Umbrella的入侵防禦系統可以檢測（並可選擇阻止）被視為與已知威脅、漏洞相關的資料包，而且只需在資料包的格式不正常時進行檢測。

管理員根據以下預設清單選擇用於檢測威脅的IPS簽名清單：

- 通過安全實現連線
- 平衡的安全和連線

- 連線安全性
- 最大檢測

請務必記住，選擇的特徵碼清單會極大地影響遇到的IPS誤報數量。最安全的模式（例如最大檢測和連線安全性）將產生不必要的IPS檢測，因為它們側重於安全性。只有在需要總體安全性時，才建議使用最安全的模式，而且管理員必須預計需要監控和檢視大量IPS事件。

有關不同模式的詳細資訊，請參閱IPS文檔。

檢視IPS檢測

使用Umbrella Dashboard上的Activity Search檢視IPS事件。對於每個事件，都有兩個重要資訊：

- IPS特徵碼ID/類別/名稱。可在https://snort.org上搜尋
- CVE編號（如果適用）。 可在https://www.cve.org/上搜尋

並非所有IPS檢測都表明存在已知漏洞/攻擊。許多特徵碼（特別是在最大檢測模式下）只表示存在某種型別的流量或協定違規。請務必檢視前面提到的資訊源以及有關事件的其他詳細資訊（如源/目標），以確定事件是否需要您的安全團隊進行進一步的調查。

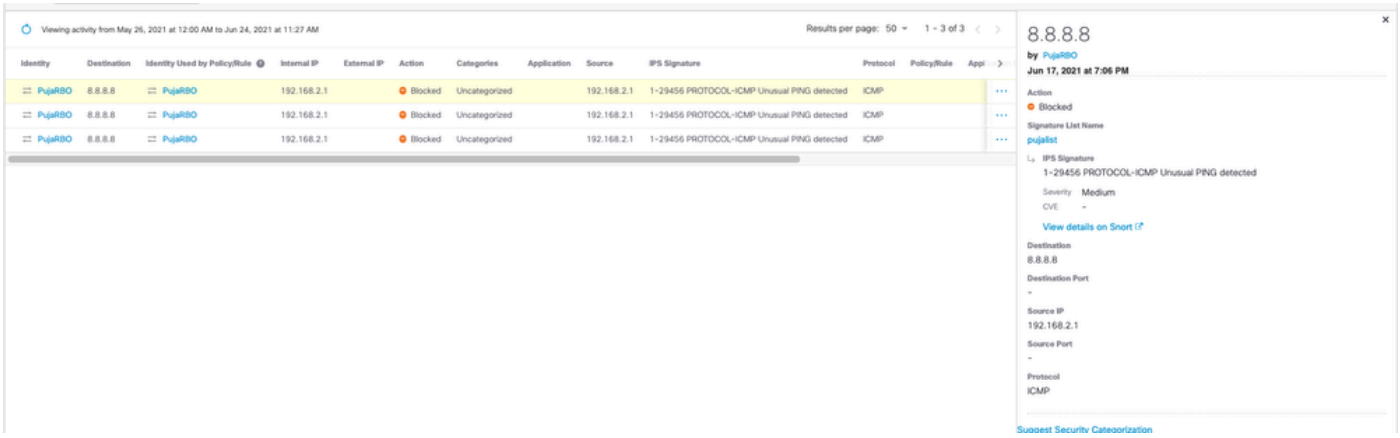
簽名類別可用於提供有關IPS檢測型別的其他上下文。檢視snort.org上提供的類別。

通訊協定違規

在本示例中，IPS事件連結到此特徵碼：
https://www.snort.org/rule_docs/1-29456

簽名的描述為：

規則查詢進入網路但不遵循PING正常格式的PING流量。



4403885889428

在這種情況下，Snort規則並不一定檢測到任何特定的利用漏洞，而是檢測到被阻止的格式錯誤的ICMP資料包。根據snort.org上可用的資訊以及有關該事件的其他詳細資訊（如源/目標），管理員可以確定不需要對此事件進行進一步的調查

應用程式相容性

某些合法應用程式與IPS特徵碼不相容，尤其是當配置了更具攻擊性（最大檢測）模式時。在這些場景中，由於協定違規部分中討論的原因，可以阻止應用程式。應用可以以一種意想不到的方式使用協定，或者通過通常為其他流量保留的埠使用自定義協定。

雖然應用是合法的，但這些檢測通常有效，且無法始終由思科進行更正。

如果合法應用程式被IPS阻止，Umbrella建議聯絡該應用程式的供應商，提供事件/特徵碼的詳細資訊。第三方應用程式必須通過snort.org測試與IPS簽名的相容性。

當前無法從IPS掃描中排除單個應用程式/目標。

禁用IPS簽名

如果發現簽名導致與第三方應用程式的相容性問題，則可以禁用簽名（臨時或永久）。 只有在您信任該應用程式，並且您確定該應用程式的價值超過了特定簽名的安全性優勢時，才能執行此操作。

完成新增自定義簽名清單文檔中的步驟，瞭解有關建立自定義簽名清單的資訊。您可以將當前設定用作模板，然後將所需規則設定為Log Only或Ignore來禁用這些規則。

支援

歷史事件

Umbrella支援無法提供有關歷史IPS事件的其他詳細資訊。IPS事件通知您流量與IPS簽名不匹配。有關簽名的詳情可公開查閱：snort.org。Umbrella不儲存原始流量/資料包的副本，因此無法提供有關IPS事件性質的進一步上下文或確認。

IPS問題/誤報

如果您希望對當前的IPS問題提出異議（例如誤報），請與Umbrella支援聯絡。

為了調查這些問題，Umbrella Support需要進行資料包捕獲。需要資料包的原始內容來確定流量如何觸發IPS檢測。您必須能夠複製問題，才能生成資料包捕獲。

在生成票證之前，使用Wireshark之類的工具在複製問題時生成資料包捕獲。 說明可以在我們的知識庫中找到。

或者，Umbrella支援可以協助生成資料包捕獲。他們需要安排時間，以便重新建立受影響的使用者或應用程式的問題。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。