用於確定每個Firepower入侵基礎策略的預設規則集的度量是什麼

目錄

簡介

Cisco Talos發佈Snort規則更新(SRU)以解決最新的威脅和漏洞。新的SRU版本可能包含每個基本策略的更新規則集。本文檔介紹Talos用來決定如何向Firepower裝置的每個入侵基礎策略分配規則的過程。

規則後設資料中定義的Talos基本策略意圖

基本策略由SRU內的後設資料維護。任何預設策略中任何給定規則的狀態在規則主體的後設資料部分中定義。例如：

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"MALWARE-CNC 1.php outbound connection
attempt"; sid:38753; gid:3; rev:1; classtype:trojan-activity; metadata:engine shared, soid
3|38753, policy balanced-ips drop, policy security-ips drop, impact_flag red; )
```

請注意，在上面的示例規則中，後設資料部分包含policy balanced-ips drop、policy security-ips drop。這表示此規則1:38753已啟用，並設定為在*Balanced Security and Connectivity*策略以及*Security over Connectivity策略*中丟棄。

用於確定預設規則集的度量

- 使用的主要度量是分配給規則可能覆蓋的每個漏洞的公共漏洞評分系統(CVSS)評分。
- 第二個度量是基於時間的，涉及特定脆弱性的年齡。
- 最終度量是規則的特定覆蓋區域。例如，SQL隱碼攻擊規則被認為足夠重要，以便在考慮策略包含時具有影響力。

附註：這些類別的規則所涵蓋的漏洞被認為重要，無論年齡大小。

基於安全基礎的連通性策略

附註：Connectivity策略專門設計用於使裝置效能優於策略中的安全控制。它應該允許客戶部署我們的裝置之一，同時儘可能減少誤報，並在大多數網路部署中保持機箱的全部額定效能。此外，此策略應檢測我們的客戶將會遇到的最常見和最常見的威脅。

1. CVSS分數必須為10

2.脆弱性來自過去兩年（包括前兩年）。 例如：

- 本年度（例如2019年）
- 去年（本例為2018年）
- 上一年（本例為2017年）

3.規則類別

- 未用於此策略

平衡基本策略

附註：Balanced策略是建議用於初始部署的預設策略。此策略試圖平衡我們的系統的安全需求和效能特性。客戶應該能夠開始使用此策略，並使用公共評估工具獲得極高的阻止率，而使用評估和測試工具則可獲得相對較高的效能率。此外，在野生網路條件下，此策略的執行速度應為裝置正常額定容量的80%。要始終牢記平衡策略的主要事項是，這是客戶的起點，如果他們誤報、檢測受限或效能較差，大多數客戶將調查在其基礎架構中部署的其他裝置。它是在Snort.org上銷售的開源Snort的Snort訂戶規則集的預設發貨狀態。

1. CVSS得分9或更高

2.脆弱性來自過去兩年（包括前兩年）。 例如：

- 本年度（例如2019年）
- 去年（本例為2018年）
- 上一年（本例為2017年）

3.規則類別

- Malware-CnC
- 黑名單
- SQL隱碼攻擊
- Exploit-kit

4.如果規則在Connectivity策略中

基於連線的安全基礎策略

附註：Security策略針對的是我們客戶群中極少數對組織安全性特別關心的人。客戶在受保護網路中部署此策略，這些網路具有較低的頻寬要求，但安全要求卻高得多。此外，客戶不太關心誤報和干擾簽名。應用控制和鎖定的網路使用也是客戶部署此策略時關心的問題。它應該提供最大的保護和應用控制，但不應使網路停機。

1. CVSS得分8或更高

2.脆弱性來自過去三年（包括前三年）。 例如：

- 本年度（例如2019年）
- 去年（本例為2018年）
- 上一年（本例為2017年）
- 上一年（本例為2016年）

3.規則類別

- Malware-CnC
- 黑名單
- SQL隱碼攻擊
- Exploit-kit

4.如果規則位於**平衡**和**連線**策略中

最大檢測（最大檢測）基本策略：

> **附註**：Maximum Detection規則集旨在用於測試環境，因此並未針對效能進行最佳化。對於此策略中的許多規則，誤報是允許和/或預期的，通常不會進行FP調查。

1.現場測試需要覆蓋範圍。

2.在**安全**、**平衡**和**連線**規則集中包含規則。

3.包括Sid上方的所有活動規則：10000，除非另有說明。

策略更新的頻率

基於這些標準，所有新規則將被置於策略中。**每年都**將對策略進行重新評估，並且隨著漏洞的年齡從策略中移除前幾年的規則，以使策略符合我們的臨時選擇標準。

如果某個規則覆蓋的特定漏洞的CVSS分數發生更改，則基於該CVSS度量的策略中是否存在該漏洞將重新進行評估。

策略不斷增長。除了進行重大調整以使它們與特定的目標保持一致以外，如果我們對產品上規則的數量和策略效能感到滿意，則不會總是發生策略的大幅刪除

> **附註**：基本策略可以隨著年度主要再平衡的增長而增長，以便與特定目標保持一致。如果Talos在正常網路條件下對產品上的規則數量和策略效能感到滿意，則不會始終發生策略中的重大規則丟棄。列出的策略中的規則將逐條規則評估。有些規則是舊規則，不在預設策略中的上述標準中。以上是預設規則的選擇標準，並且始終會根據威脅狀況而發生更改。

> **註**：所列策略中的規則將逐條規則評估。有些規則是舊規則，不在預設策略中的上述標準中。以上是預設規則的選擇標準，並且始終會根據威脅狀況而發生更改