Anhand welcher Metriken wird die Standardregel für jede Richtlinie für Firepower Intrusion Base ermittelt?

Inhalt

Einführung

Cisco Talos veröffentlicht Snort Rule Updates (SRU), um auf die neuesten Bedrohungen und Schwachstellen einzugehen. Eine neue SRU-Version kann aktualisierte Regeln für jede Basisrichtlinie enthalten. In diesem Dokument wird der Prozess erläutert, mit dem die Talos entscheiden, wie Regeln den Intrusion Base-Richtlinien für FirePOWER-Geräte zugewiesen werden.

In Regelmetadaten definierte Talos-Basisrichtlinie

Die Basisrichtlinien werden von Metadaten in den SRUs selbst verwaltet. Der Zustand einer bestimmten Regel in einer der Standardrichtlinien wird im Metadatenbereich des Regelkörpers definiert. Beispiel:

```
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; )
```

In der obigen Beispielregel ist zu beachten, dass der Metadatenbereich Policy Balancing-ips Drop, Policy Security-ips Drop enthält.Dies bedeutet, dass diese Regel 1:38753 aktiviert ist und in der *Balanced Security and Connectivity-Richtlinie* sowie in der *Security Over Connectivity-Richtlinie* verworfen wird.

Kennzahlen zur Bestimmung der Standardregeln

- Die wichtigste Kennzahl ist das Common Vulnerability Scoring System (CVSS)-Ergebnis, das jeder Schwachstelle zugewiesen ist, die von einer Regel abgedeckt werden könnte.
- Die zweite Kennzahl ist zeitbasiert und bezieht sich auf das Alter einer bestimmten Schwachstelle.

- Die letzte Kennzahl ist der spezielle Abdeckungsbereich für die Regel. So werden beispielsweise SQL-Injection-Regeln als wichtig genug angesehen, um Einfluss zu haben, wenn sie für die Einbeziehung von Richtlinien in Betracht gezogen werden.

  Hinweis: Die von den Regeln in diesen Kategorien erfassten Schwachstellen werden unabhängig vom Alter als wichtig angesehen.

Konnektivität über Basis-Sicherheitsrichtlinie

Hinweis: Die **Connectivity-**Richtlinie wurde speziell entwickelt, um die Geräteleistung gegenüber den Sicherheitskontrollen in der Richtlinie zu fördern. Sie sollte es dem Kunden ermöglichen, eines unserer Geräte mit minimalen Fehlalarmen und einer voll bewerteten Leistung in den meisten Netzwerkbereitstellungen bereitzustellen. Darüber hinaus sollte diese Richtlinie die häufigsten und häufigsten Bedrohungen erkennen, die unsere Kunden erwarten.

1. CVSS-Bewertung muss 10 sein.

2. Die Schwachstelle ist seit den letzten zwei Jahren (einschließlich) entstanden. Beispiel:

   - Aktuelles Jahr (z. B. 2019)
   - Letztes Jahr (in diesem Beispiel 2018)
   - Jahr vor dem letzten (in diesem Beispiel 2017)
3. Regelkategorie

   - Nicht für diese Richtlinie verwendet

Ausgewogene Basisrichtlinie

Hinweis: Die **Balanced-**Richtlinie ist die Standardrichtlinie, die für die Erstbereitstellung empfohlen wird. Diese Richtlinie versucht, Sicherheitsanforderungen und Leistungsmerkmale unserer Systeme miteinander in Einklang zu bringen. Kunden sollten mit dieser Richtlinie beginnen und eine sehr gute Blockierungsrate mit öffentlichen Evaluierungstools und eine relativ hohe Performance mit Evaluations- und Testtools erzielen können. Zusätzlich sollte diese Richtlinie unter normalen Netzwerkbedingungen 80 % der Nennkapazität des Geräts ausmachen. Bei der Balanced-Richtlinie sollten Sie vor allem beachten, dass dies der Ausgangspunkt des Kunden ist. Wenn der Kunde schlechte Erfahrungen mit Fehlalarmen, eingeschränkter Erkennung oder schlechter Leistung hat, werden die meisten Kunden andere Geräte für die Bereitstellung in seiner Infrastruktur untersuchen. Dies ist der Standardversandzustand des Snort Subscriber Rule Set für Open-Source Snort, der auf Snort.org verkauft wird.

1. CVSS Score 9 oder höher

2. Die Schwachstelle ist seit den letzten zwei Jahren (einschließlich) entstanden. Beispiel:

- Aktuelles Jahr (z. B. 2019)
- Letztes Jahr (in diesem Beispiel 2018)
- Jahr vor dem letzten (in diesem Beispiel 2017)

3. Regelkategorie

   - Malware-CnC
   - Blacklist
   - SQL-Injection
   - Exploit-Kit

4. Wenn die Regel in der **Connectivity-**Richtlinie enthalten ist

Grundlegende Richtlinie für Sicherheit über Konnektivität

> **Hinweis**: Die **Security** Policy wurde für kleine Teile unseres Kundenstamms entwickelt, die sich außerordentlich um die Sicherheit der Organisation sorgen. Kunden implementieren diese Richtlinie in geschützten Netzwerken, die geringere Bandbreitenanforderungen, aber deutlich höhere Sicherheitsanforderungen haben. Darüber hinaus sorgen sich Kunden weniger um Fehlalarme und geräuschlose Signaturen. Die Anwendungskontrolle und die Sperrung der Netzwerknutzung stellen ebenfalls Bedenken bei Kunden dar, die diese Richtlinie implementieren. Sie sollte einen maximalen Schutz und eine optimale Anwendungskontrolle bieten, jedoch nicht zum Ausfall des Netzwerks führen.

1. CVSS Score 8 oder höher

2. Die Schwachstelle ist seit drei Jahren (einschließlich) entstanden. Beispiel:

   - Aktuelles Jahr (z. B. 2019)
   - Letztes Jahr (in diesem Beispiel 2018)
   - Jahr vor dem letzten (in diesem Beispiel 2017)
   - Vorjahr (in diesem Beispiel 2016)

3. Regelkategorie

   - Malware-CnC
   - Blacklist
   - SQL-Injection
   - Exploit-Kit

4. Wenn die Regel in der **Balanced** and **Connectivity-**Richtlinie enthalten ist

Max-Detect (Maximum Detect)-Basisrichtlinie:

> **Hinweis**: Die **Maximum Detection**-Regeln sind für Testumgebungen vorgesehen und sind daher nicht leistungsoptimiert. Fehlalarme für viele Regeln dieser Politik werden toleriert und/oder erwartet, und FP-Untersuchungen werden normalerweise nicht durchgeführt.

1. Die Abdeckung ist für Vor-Ort-Tests erforderlich.

2. Enthält Regeln für die Regelsätze **Sicherheit**, **Ausgewogenes** und **Konnektivität**.

3. Beinhaltet alle aktiven Regeln über Sid: 10000, sofern nicht anders angegeben.

Häufigkeit der Richtlinien-Updates

Alle neuen Regeln werden auf der Grundlage dieser Kriterien in die Richtlinien eingefügt. **Die** Richtlinien werden **jedes Jahr** neu bewertet, und die Regeln der vergangenen Jahre werden, da die Sicherheitslücken älter werden, aus der Richtlinie entfernt, damit die Richtlinie unseren Kriterien für die zeitliche Auswahl entspricht.

Wenn sich der CVSS-Wert für eine bestimmte Schwachstelle ändert, die von einer Regel abgedeckt wird, wird das Vorhandensein dieser Schwachstelle in einer Richtlinie, die auf der CVSS-Metrik basiert, neu bewertet.

Richtlinien wachsen kontinuierlich. Abgesehen von einer größeren Neuausrichtung, um sie an ein bestimmtes Ziel auszurichten, kommt es nicht immer zu großen Regelverlusten aus der Politik, wenn wir mit der Anzahl der Regeln und der Leistung der Produktpolitik zufrieden sind

> **Hinweis**: Basispolitische Maßnahmen können von der jährlichen größeren Neugewichtung abweichen, um sie an ein bestimmtes Ziel auszurichten. Große Regelverluste aus Richtlinien treten nicht immer auf, wenn Talos mit der Anzahl der Regeln und der Leistung der Richtlinie für das Produkt unter normalen Netzwerkbedingungen zufrieden ist. Regeln in den aufgelisteten Richtlinien werden regelabhängig evaluiert. Es gibt einige Regeln, die älter sind und nicht in den obigen Kriterien enthalten sind, die in den Standardrichtlinien enthalten sind. Bei den oben aufgeführten Kriterien handelt es sich um die Auswahlkriterien für Standardregeln, die sich je nach Bedrohungslandschaft ändern können.

> **Hinweis**: Regeln in den aufgelisteten Richtlinien werden regelabhängig evaluiert. Es gibt einige Regeln, die älter sind und nicht in den obigen Kriterien enthalten sind, die in den Standardrichtlinien enthalten sind. Bei den oben aufgeführten Kriterien handelt es sich um die Auswahlkriterien für Standardregeln, die sich je nach Bedrohungslandschaft ändern können.