ما هي المقاييس المستخدمة لتحديد القواعد الافتراضية لكل سياسة أساسية لاقتحام قوة النار

المحتويات

المقدمة

يطلق Cisco Talos تحديثات قاعدة snort (SRU) لمعالجة أحدث التهديدات ومكامن الضعف. قد يحتوي إصدار SRU جديد على قواعد محدثة لكل سياسة أساسية. يشرح هذا المستند العملية التي يستخدمها Talos لتحديد كيفية تخصيص القواعد لكل سياسة قاعدة إقتحام لأجهزة FirePOWER.

تم تعريف "هدف النهج الأساسي لـ Talos" في بيانات تعريف القاعدة

ويتم الحفاظ على السياسات الأساسية عن طريق البيانات الوصفية داخل وحدات تمثيل الموظفين نفسها. يتم تعريف حالة أي قاعدة "منح" في أي من النهج الافتراضية في جزء بيانات التعريف من نص القاعدة. على سبيل المثال:

```
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; )
```

لاحظ أنه في قاعدة المثال الموضحة أعلاه، يحتوي قسم بيانات التعريف على **إسقاط IPS** و**تعيينها 1:38753 القاعدة هذه إلى تمكين يشير هذا إلى النهج المتوازن للنهج والإفلات من الآمن للنهج**. بالإضافة إلى *نهج الأمان عبر الاتصال* في *نهج الأمان المتوازن والاتصال* للإفلات.

المقاييس المستخدمة لتحديد القواعد الافتراضية

- المقياس الرئيسي المستخدم هو علامة نظام تسجيل نقاط الضعف الشائعة (CVSS) المخصصة لكل نقطة ضعف قد تغطيها قاعدة ما.
- والمقياس الثاني هو قياس زمني ويتعلق بعمر ضعف معين.
- والمقياس النهائي هو مجال التغطية المحدد للقاعدة. على سبيل المثال، تعتبر قواعد

حقن SQL مهمة بما يكفي ليكون لها تأثير عند النظر في إدراجها في السياسة.

ملاحظة: تعتبر أوجه الضعف التي تغطيها القواعد في هذه الفئات هامة بغض النظر عن العمر.

الاتصال عبر سياسة قاعدة الأمان

ملاحظة: صممت سياسة **الاتصال** خصيصا لتفضيل أداء الجهاز على عناصر التحكم في الأمان في السياسة. يجب أن تسمح لأي عميل بنشر أحد أجهزتنا بأقل قدر ممكن من الإيجابيات الخاطئة والأداء المقدر الكامل للجهاز في معظم عمليات نشر الشبكة. بالإضافة إلى ذلك، يجب أن تكشف هذه السياسة عن التهديدات الأكثر شيوعا والأكثر انتشارا التي سيتعرض لها عملاؤنا.

1. يجب أن تكون درجة CVSS 10

2 - وقد بدأ الضعف في العامين الأخيرين (شامل). على سبيل المثال:

- السنة الحالية (2019 على سبيل المثال)
- العام الماضي (2018 في هذا المثال)
- السنة التي تسبق السنة الماضية (2017 في هذا المثال)

3. فئة القاعدة

- غير مستخدم لهذا النهج

سياسة الأساس المتوازن

ملاحظة: السياسة **المتوازنة** هي السياسة الافتراضية الموصى بها لعمليات النشر الأولية. تحاول هذه السياسة تحقيق التوازن بين إحتياجات الأمان وخصائص الأداء لأنظمتنا. يجب أن يكون العملاء قادرين على البدء بهذا النهج والحصول على معدل حظر جيد جدا باستخدام أدوات التقييم العامة ومعدل أداء مرتفع نسبيا من خلال أدوات التقييم والاختبار. بالإضافة إلى ذلك، يجب أن تعمل هذه السياسة بنسبة 80٪ من السعة المقدرة للجهاز في الظروف العادية للشبكات البريئة. إن الشيء الرئيسي الذي يجب وضعه في الاعتبار دائما مع السياسة المتوازنة هو أنها تمثل نقطة بداية العملاء، إذا كانت لديهم تجربة سيئة مع الإيجابيات الكاذبة أو الكشف المحدود أو الأداء الضعيف، فمعظم العملاء سيبحثون عن أجهزة أخرى للنشر في البيئة الأساسية لديهم. إنها حالة الشحن الافتراضية لقاعدة المشترك في برنامج Snort التي تم تعيينها لـ Open-Source Snort التي يتم بيعها على Snort.org.

1. درجة CVSS 9 أو أعلى

2 - وقد بدأ الضعف في العامين الأخيرين (شامل). على سبيل المثال:

- السنة الحالية (2019 على سبيل المثال)
- العام الماضي (2018 في هذا المثال)
- السنة التي تسبق السنة الماضية (2017 في هذا المثال)

3. فئة القاعدة

- Malware-CNc
- عادوس قائمة
- حقن SQL
- مجموعة أدوات الاستغلال

4. إذا كانت القاعدة موجودة في نهج **الاتصال**

الأمان عبر سياسة قاعدة الاتصال

> **ملاحظة**: تم تصميم سياسة **الأمان** للجزء الصغير من قاعدة عملائنا الذي يهتم بشكل إستثنائي بالأمان التنظيمي. يقوم العملاء بنشر هذا النهج في الشبكات المحمية التي تتميز بمتطلبات عرض نطاق ترددي أقل ولكنها متطلبات أمان أعلى بكثير. بالإضافة إلى ذلك، يهتم العملاء بشكل أقل بالإثباتات الإيجابية الخاطئة والتواقيع الصاخبة. التحكم في التطبيقات واستخدام الشبكة المؤمنان هما أيضا من شواغل العملاء الذين يقومون بنشر هذا النهج. يجب أن توفر أقصى قدر من الحماية والتحكم في التطبيقات، ولكن لا يجب أن تتسبب في تعطيل الشبكة.

1. درجة CVSS 8 أو أعلى

2 - وقد بدأ الضعف في السنوات الثلاث الأخيرة (شاملة). على سبيل المثال:

- السنة الحالية (2019 على سبيل المثال)
- العام الماضي (2018 في هذا المثال)
- السنة التي تسبق السنة الماضية (2017 في هذا المثال)
- السنة السابقة (2016 في هذا المثال)

3. فئة القاعدة

- Malware-CNc
- عادوس قائمة
- حقن SQL
- مجموعة أدوات الاستغلال

4. إذا كانت القاعدة موجودة في نهج **التوازن والاتصال**

نهج قاعدة الكشف الأقصى:

> **ملاحظة**: يقصد **من قواعد الكشف الأقصى** أن تستخدم في بيئات الاختبار، ومن ثم فهي غير محسنة للأداء. ويجري التسامح مع العديد من القواعد الواردة في هذه السياسة و/أو توقع نتائج إيجابية زائفة، كما أن التحقيقات التي يجريها مكتب المدعي العام لا تجرى عادة.

1 - التغطية مطلوبة للاختبارات الميدانية.

2. يتضمن القواعد في مجموعات قواعد **الأمان والمتوازن والاتصال**.

3 - يشمل جميع القواعد النشطة الواردة فوق SID: 10000، ما لم ينص على خلاف ذلك.

تكرار تحديثات النهج

وتدرج جميع القواعد الجديدة في السياسات القائمة على هذه المعايير. **وفي كل عام** سوف يعاد تقييم السياسات وسوف يتم حذف القواعد من الأعوام السابقة، مع تقدم سن نقاط الضعف، من هذه السياسة إلى السياسة متوافقة مع معايير الاختيار الزمنية.

إذا تم تغيير درجة CVSS لضعف معين تغطيه قاعدة، فإنه يتم إعادة تقييم وجوده في سياسة قائمة على مقياس CVSS.

والسياسات تنمو باستمرار. وبعيدا عن عملية إعادة التوازن الرئيسية لمواءمتها مع هدف محدد، فإن حالات هبوط القواعد في السياسات لا تحدث دوما إذا كنا راضين عن عدد القواعد وأداء السياسة فيما يتصل بالمنتج

ملاحظة: يمكن أن تنمو السياسات الأساسية بشكل منفصل عن عملية إعادة التوازن الرئيسية السنوية لتتواءم مع هدف محدد. لا تحدث دائما حالات إسقاط القواعد بشكل كبير من السياسات إذا كان Talos راضيا عن عدد القواعد وأداء السياسة على المنتج في ظل ظروف الشبكة العادية. يتم تقييم القواعد في السياسات المدرجة على أساس قاعدة قاعدة. سوف تكون هناك بعض القواعد الأقدم وليس في المعايير أعلاه والتي سوف تكون في السياسات الافتراضية. والمذكور أعلاه هو معايير إختيار القواعد الافتراضية، وهي عرضة دائما للتغيير استنادا إلى مشهد التهديد.

ملاحظة: يتم تقييم القواعد في السياسات المدرجة على أساس قاعدة قاعدة. سوف تكون هناك بعض القواعد الأقدم وليس في المعايير أعلاه والتي سوف تكون في السياسات الافتراضية. والمذكور أعلاه هو معايير إختيار القواعد الافتراضية، وهي عرضة دائما للتغيير بناء على مشهد التهديد

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).