مراجعة نتائج IPS الإيجابية الخاطئة مع Umbrella أو النزاع عليها

المحتويات

المقدمة

يوضح هذا المستند كيفية مراجعة نتائج إيجابية خاطئة لخدمة منع التسلل (IPS) أو التنازع عليها باستخدام Cisco Umbrella.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى Cisco Umbrella.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

نظرة عامة

يقوم نظام Cisco Umbrella لمنع الاقتحام باكتشاف الحزم (وحظرها إختياريا) التي تم اعتبارها مرتبطة بتهديد معروف، ومكامن الضعف، ولكن ببساطة أيضا عندما يكون تنسيق الحزمة غير عادي.

يختار المسؤولون قائمة توقيع IPS التي يتم إستخدامها لاكتشاف التهديدات استنادا إلى هذه القوائم الافتراضية:

- الاتصال عبر الأمان
- إمكانات اتصال وأمان متوازنة
- الأمان عبر الاتصال
- الحد الأقصى للكشف

من المهم تذكر أن قائمة التوقيع المختارة يمكن أن تؤثر بشكل كبير على عدد الإيجابيات الخاطئة ل IPS التي تمت مواجهتها. من المتوقع أن تووم الأوضاع الأكثر أمانا (مثل الاكتشاف الأقصى والأمان عبر الاتصال) بإنشاء عمليات اكتشاف IPS غير المرغوب فيها لأنها تركز على الأمان. الى يوصى بالأوضاع الأكثر أمانا إلا في حالة الحاجة إلى توفير أمان كامل، كما يجب على المسؤول توقع الحاجة إلى مراقبة أعداد كبيرة من أحداث IPS ومراجعتها.

لمزيد من المعلومات حول الأوضاع المختلفة، راجع وثائق IPS.

مراجعة اكتشافات IPS

أستخدم "البحث عن النشاط" على لوحة معلومات المظلة لعرض أحداث IPS. تتوفر لكل حدث معلومتان مهمتان:

- معرف/فئة/اسم توقيع IPS. يمكن البحث فيه على https://snort.org
- رقم CVE (إن أمكن). يمكن البحث فيه على https://www.cve.org/

ال تشير جميع عمليات الكشف عن العبوات النافذة الداخلية إلى وجود عملية إستغلال/هجوم معروفة. كثير من التوقيعات (خاصة في وضع الكشف الأقصى) ببساطة يشير إلى وجود نوع معين من حركة المرور، أو بروتوكول انتهاك. من المهم مراجعة مصادر المعلومات التي تمت الإشارة إليها سابقا مع التفاصيل الأخرى المتعلقة بالحدث (مثل المصدر/الوجهة) لتحديد ما إذا كان الحدث يتطلب مزيدا من التحقيق من قبل فريق الأمن التابع لك.

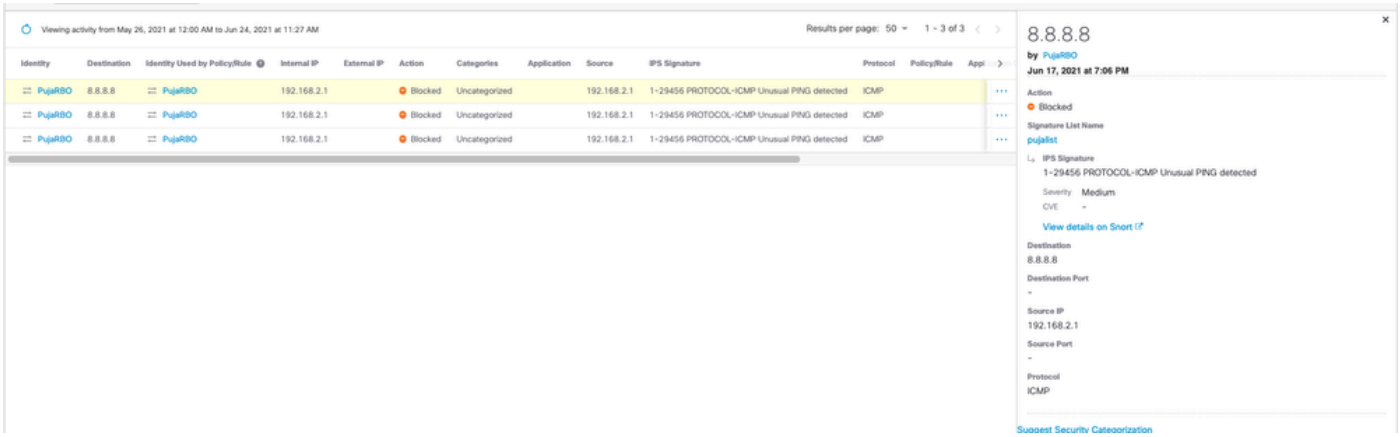
يمكن أن تكون فئة التوقيع مفيدة في توفير سياق إضافي حول نوع كشف IPS. راجع الفئات المتوفرة على موقع الويب snort.org.

انتهاكات البروتوكول

في هذا المثال، يتم رطب حدث IPS بهذا التوقيع :
https://www.snort.org/rule_docs/1-29456

وصف التوقيع هو:

"تبحث القاعدة عن حركة مرور PING القادمة إلى الشبكة التي ال تتبع التنسيق العادي ل PING."



4403885889428

في هذه الحالة، ال تكون قاعدة الشرخ بالضرورة تكشف عن أي إستغلال معين، ولكنها توقم ICMP مكونة بشكل غير صحيح تم حظرها. بناء على المعلومات المتوفرة على موقع الويب snort.org وتفاصيل أخرى حول الحدث (مثل المصدر/الوجهة)، يمكن أن يقرر المسؤول أن هذا الحدث ال يتطلب مزيدا من التحقيق

توافق التطبيقات

ال تتوافق بعض التطبيقات الشرعية مع توقيعات IPS، خاصة عند تكوين الأوضاع الأكثر عدوانية (الكشف الأقصى). في هذه السيناريوهات، يمكن حظر التطبيق للأسباب التي تمت مناقشتها في قسم انتهاك البروتوكول. يمكن للتطبيق إستخدام بروتوكول بطريقة غير متوقعة، أو إستخدام بروتوكول مخصص عبر منفذ ما يكون عادة محجوزا لحركة مرور أخرى.

على الرغم من أن التطبيق مشروع، إلا أن هذه عمليات الكشف غالبا ما تكون صحيحة ولا يمكن تصحيحها دائما بواسطة Cisco.

إذا تم حظر تطبيق شرعي من قبل IPS، توصي Umbrella بالاتصال بمورد التطبيق مع تفاصيل الحدث/التوقيع. يجب إختبار تطبيقات الجهات الخارجية للتوافق مع توقيعات نظام منع التسلل (IPS) على العنوان snort.org.

ال يمكن حاليا إستبعاد تطبيق/وجهة منفردة من مسح IPS.

تعطيل توقيعات IPS

إذا وجد توقيع أن يسبب مشاكل توافق مع تطبيق خارجي، التوقيع يمكن أن يكون معأق (إما مؤقتا أو دائما). يجب أن يتم ذلك فقط عندما تكون واثقا من التطبيق وقد قررت أن قيمة التطبيق تفوق فوائد الأمان الخاصة بالتوقيع المحدد.

قم بإكمال الخطوات في [إضافة قائمة توقيع مخصصة وإنشاء قائمة](#) لمعلومات عن إنشاء قائمة توقيع مخصصة. يمكنك إستخدام إعداداتك الحالية كقالب ثم تعطيل القواعد المطلوبة عن طريق تعيينها على تسجيل الدخول فقط أو تجاهل.

الدعم

أحداث تاريخية

يتعذر على "دعم Umbrella" توفير تفاصيل إضافية حول أحداث IPS التاريخية. تخبرك أحداث IPS بأن حركة المرور لم تتطابق مع توقيع IPS. () تفاصيل التوقيع متاحة للجمهور على الموقع snort.org. الـ Umbrella تخزين نسخة من حركة المرور/الحزم الخام، ومن ثم فإنها غير قادرة على توفير سياق إضافي أو تأكيد حول طبيعة حدث IPS.

مشاكل IPS / الإيجابيات الخاطئة

إذا كنت ترغب في النزاع حول مشكلة IPS حالية (مثل نتيجة إيجابية خاطئة)، فيرجى الاتصال بدعم Umbrella.

للتحقيق في هذه المشاكل، يلزم التقاط حزمة بواسطة دعم Umbrella. يلزم وجود المحتويات الأولية للحزم لتحديد كيفية تشغيل حركة المرور لاكتشاف IPS. أنت ينبغي كنت يمكن أن يكرر الإصدار in order to خلق التقاط الربط.

قبل رفع تذكرة، أستخدم أداة مثل Wireshark لتوليد التقاط الحزمة عند نسخ الإصدار. التعليمات متوفرة في قاعدة معارفنا.

بدلا من ذلك، يمكن أن يساعد دعم Umbrella في إنشاء التقاط الحزمة. تحتاج إلى جدولة الوقت الذي يمكن فيه إعادة إنشاء المشكلة مع المستخدم أو التطبيق المتأثر.

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).