أستخدم "إطار عمل MITER" لعرض التهديدات المحتملة في وحدة التحكم في إدارة اللوحة الأساسية (FMC) الآمنة والعمل على التصدي لها

المحتويات

المقدمة

يوضح هذا المستند كيفية إستخدام إطار عمل MITER لعرض التهديدات المحتملة والعمل عليها في مركز إدارة FirePOWER الآمن (FMC).

معلومات أساسية

إن إطار عمل "ميتر آند كي" (التكتيكات العدائية والتقنيات والمعارف المشتركة) هو قاعدة معرفية ومنهجية واسعة النطاق توفر رؤى ثاقبة حول التكتيكات والتقنيات والإجراءات (TTPs) التي يتم توزيعها من قبل الجهات الفاعلة في التهديدات التي تهدف إلى إلحاق الضرر بالأنظمة. وتجمع ATT&CK في مصفوفات تمثل كل منها نظم تشغيل أو منصة معينة. كل مرحلة من مراحل الهجوم تعرف ب "التكتيك" ويكون معتمدا على الأساليب المحددة المستخدمة في تحقيق تلك المراحل، والمعروفة باسم "الأساليب".

وكل تقنية في إطار إتفاق التجارة في الخدمات والصكوك تصحبها معلومات عن التقنية، والإجراءات المرتبطة بها، والدوفع المحتملة، وعمليات الكشف، وأمثلة من العالم الحقيقي. كما أن إطار عمل "ميتر آند كي" يضم أيضا جماعات للإشارة إلى جماعات التهديد أو مجموعات الأنشطة أو الجهات الفاعلة في مجال التهديد استنادا إلى مجموعة من التكتيكات والتقنيات التي تستخدمها. باستخدام المجموعات، يساعد إطار العمل على تصنيف سلوكيات المستندات.

لمزيد من المعلومات حول Miter، يرجى الرجوع إلى https://attack.mitre.org.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة الشيخ
- FMC آمن
- الدفاع الآمن عن تهديد قوة الحماية (FTD)

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- ينطبق هذا المستند على جميع منصات Firepower
- برنامج Secure FTD الجاري تشغيله، الإصدار 7.3.0
- Secure Firepower Management Center Virtual (FMC) الذي يشغل الإصدار 7.3.0 من البرنامج

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.

فوائد إطار عمل ميتر

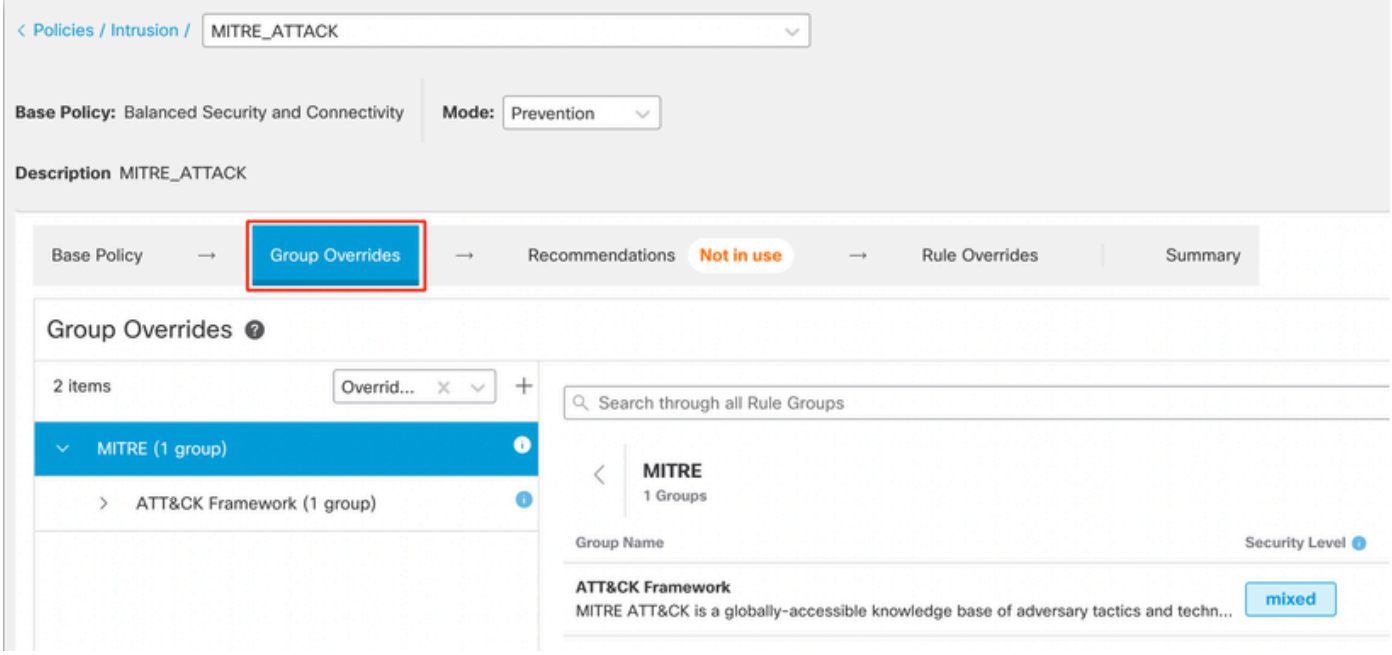
- تتم إضافة تكتيكات وتقنيات وإجراءات نقل البيانات إلى أحداث التسلل التي تمكن المسؤولين من العمل بناء على إطار عمل MITER ATT&CK (تكتيكات الخصم والمعارف الشائعة). وهذا يمكن المسؤولين من عرض حركة المرور ومعالجتها بمزيد من القابلية للتعديل، كما يمكنهم تجميع القواعد حسب نوع الثغرات أو النظام الهدف أو فئة التهديد.
- يمكنك تنظيم قواعد التطفل وفقا لإطار عمل "ميتر إيه تي أند كيه". وهذا يسمح لك بتخصيص السياسات وفقا لتكتيكات وتقنيات مهاجمين معينة.

عرض إطار عمل MITER في نهج التسلل

يمكن إطار عمل MITER من التنقل خلال قواعد التطفل الخاصة بك. وميتر هو مجرد فئة أخرى من مجموعات القواعد وهو جزء من مجموعات قواعد Talos. تنقل القواعد لعدة مستويات من مجموعات القواعد مدعوم مما يوفر مرونة أكبر وتجميع منطقي للقواعد.

1. أخترPolicies > Intrusion.
2. تأكد من إختيارIntrusion Policiesعلامة التبويب.
3. انقرSnort 3 Versionبجوار سياسة التطفل التي تريد عرضها أو تحريرها. أغلق دليل مساعد النخر الذي يظهر.
4. انقر فوقGroup Overridesالطبقة.

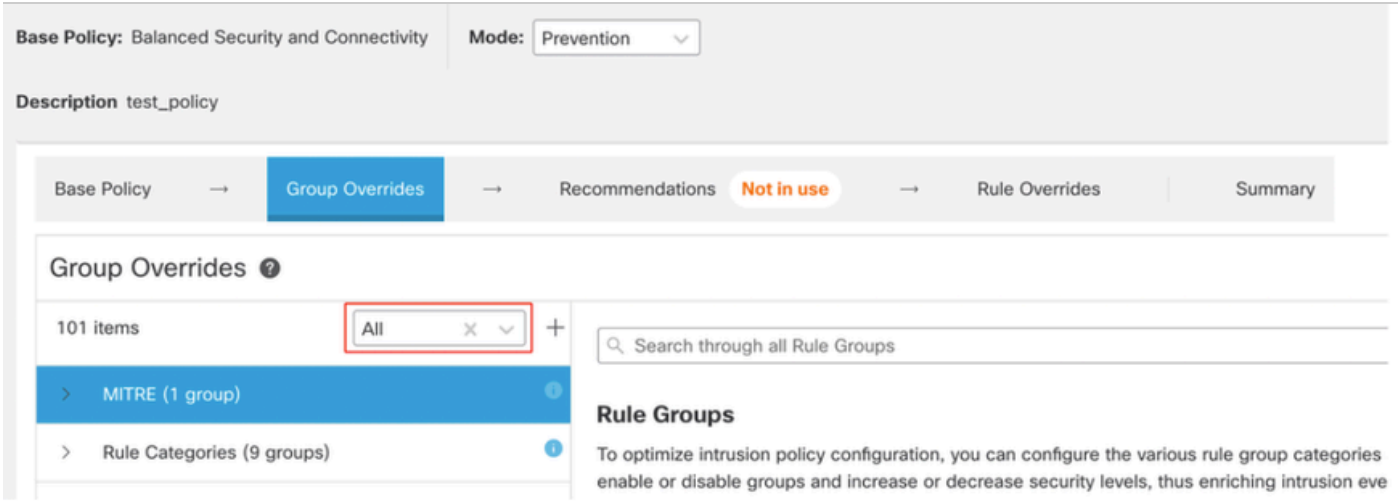
تسردGroup Overridesالطبقة كل فئات مجموعات القواعد في هيكل هرمي. يمكنك إجتياز المجموعة الأخيرة لمسطرة الورقة في كل مجموعة قاعدة.



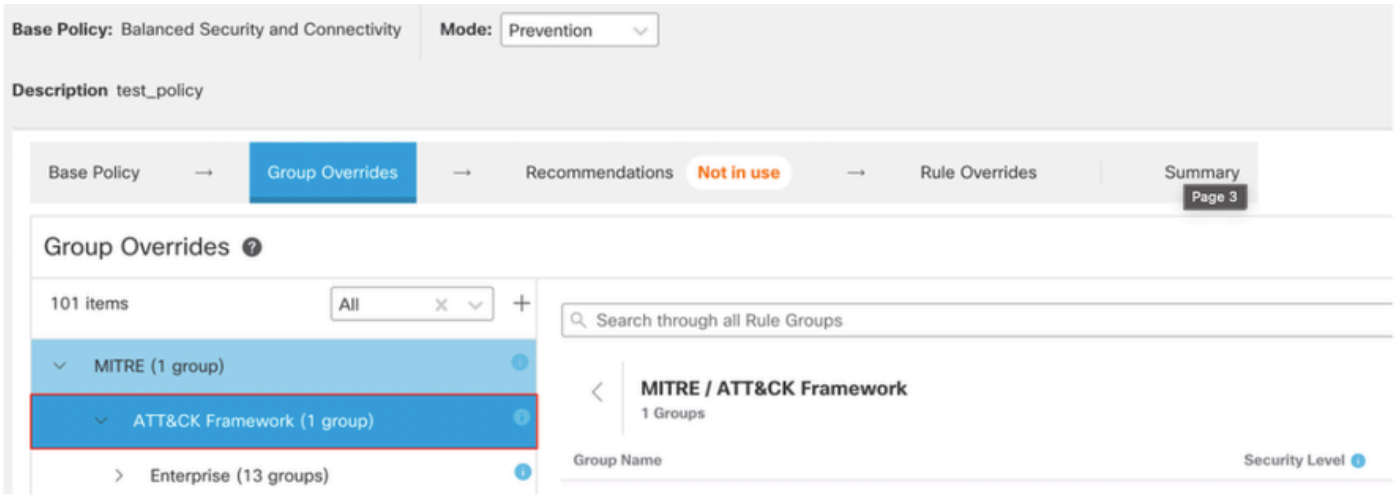
6 -Group Overridesفي إطار البند، كفالة ما يلي Allفي القائمة المنسدلة، بحيث تكون كافة مجموعات القواعد لنهج التطفل مرئية في الجزء الأيسر.

7. انقر MITREفي الجزء الأيسر.

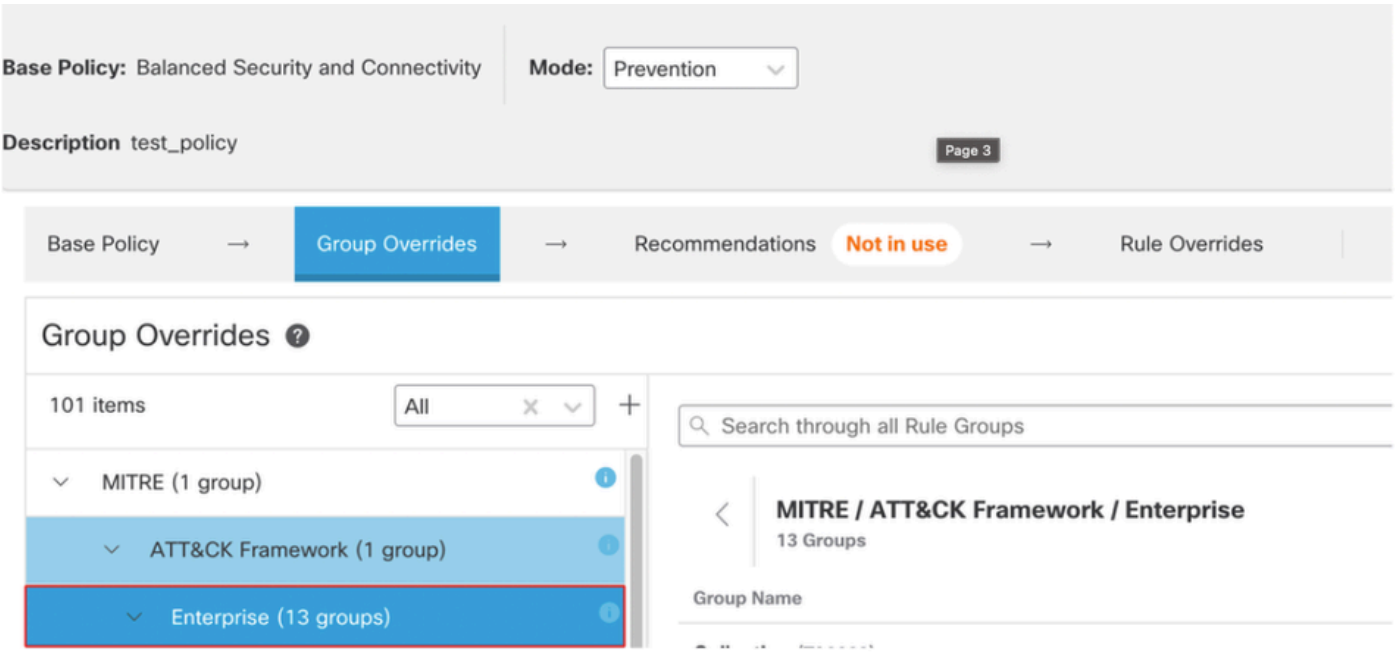
ملاحظة: على سبيل المثال، تم تحديد MITER، ولكن بناء على متطلباتك الخاصة، يمكنك إختيار مجموعة قواعد فئات القاعدة أو أي مجموعة قواعد أخرى ومجموعات قواعد تالية تحتها. تستخدم كافة مجموعات القواعد إطار عمل MITER.



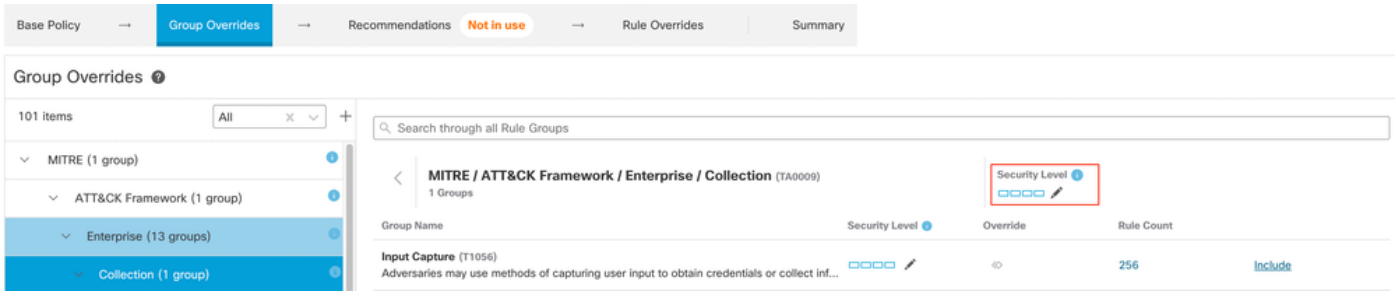
8. تحتMITRE، انقر فوق إطارATT&CKلعمل لتمديده.



9. تحتATT&CK Framework، انقر فوق "مؤسسة" لتمديده.

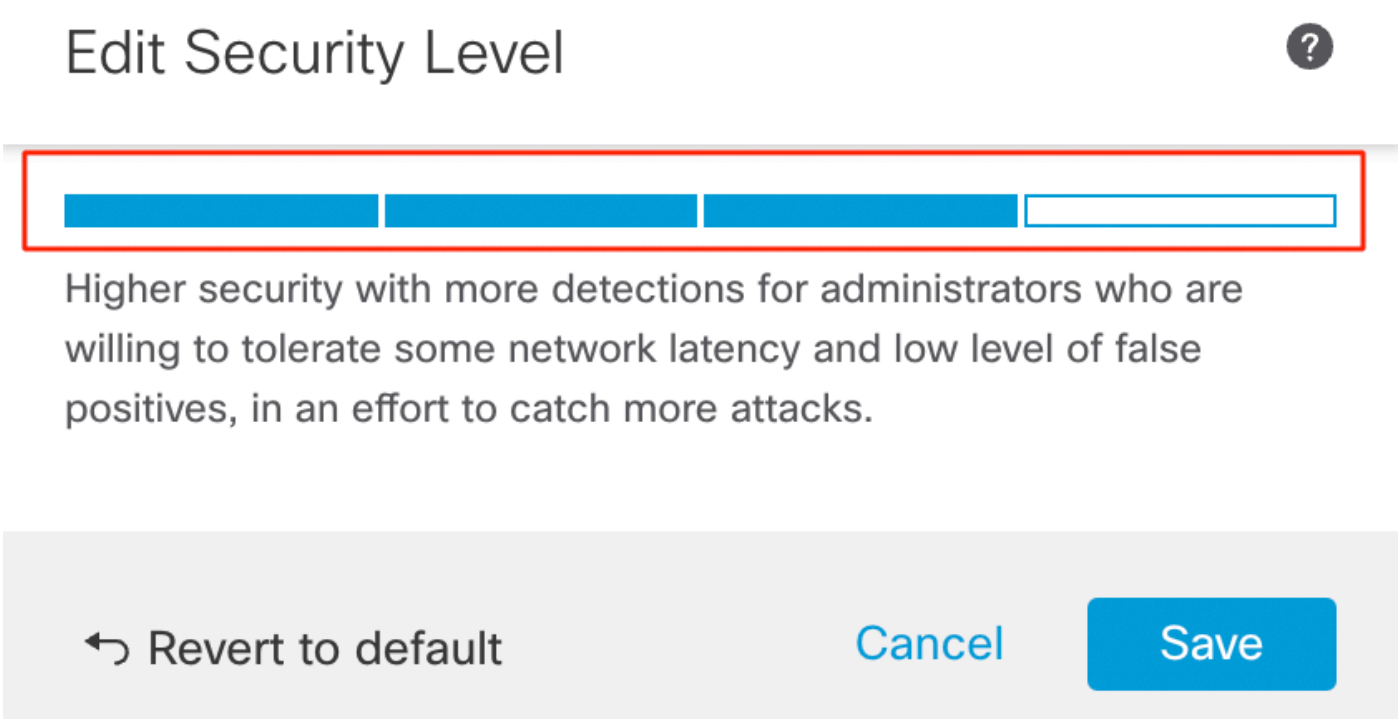


10. انقرEdit ( ) بجوار مستوى الأمان لمجموعة القواعد لإجراء تغييرات كبيرة على مستوى الأمان لكافة مجموعات القواعد المقترنة ضمن Enterpriseفئة مجموعة القواعد.



تحرير مجموعة قواعد الأمان

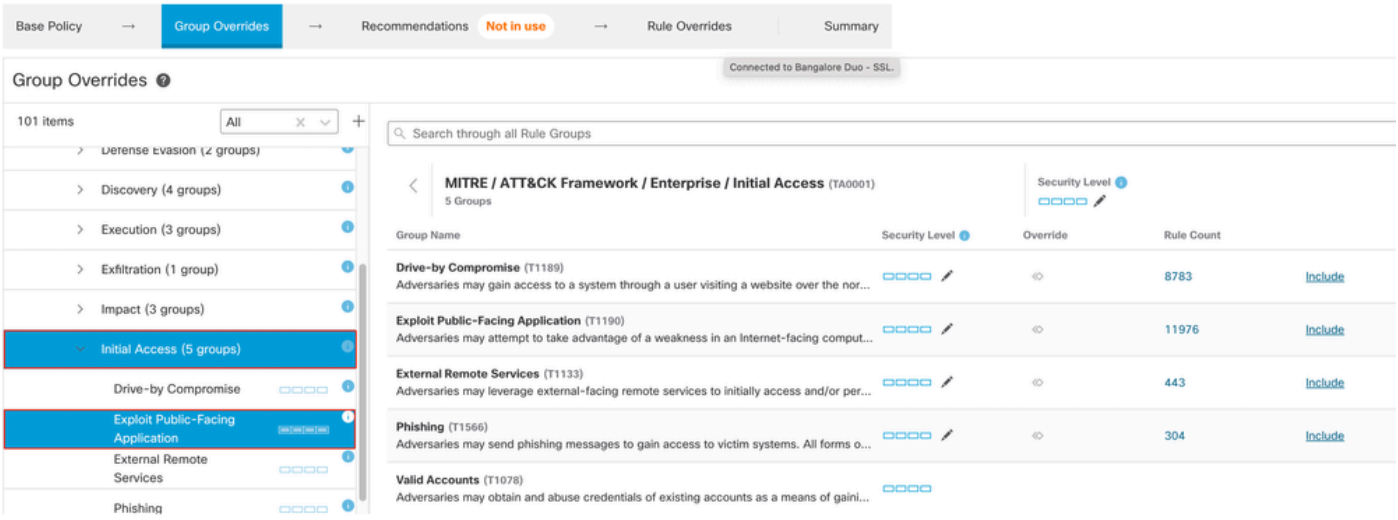
11. على سبيل المثال، أختر مستوى الأمان 3 فيEdit Security Levelالإطار وانقر **Save**.



مستوى الأمان

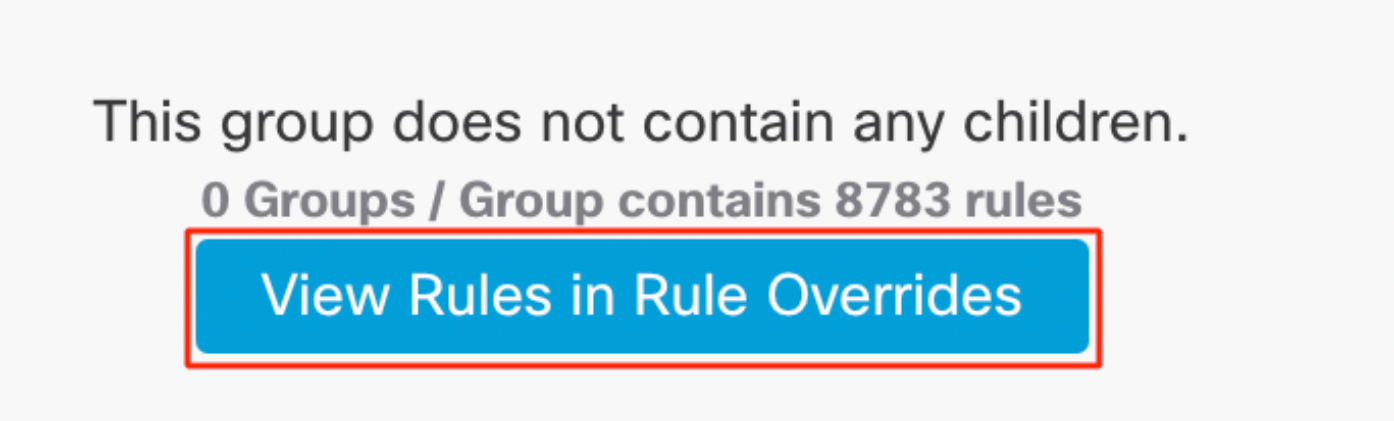
12. تحتEnterprise، انقر Initial Accessلتوسيع نطاقه.

13. تحتInitial Access، انقرExploit Public-Facing Application، والتي هي المجموعة الأخيرة من الصفحات.



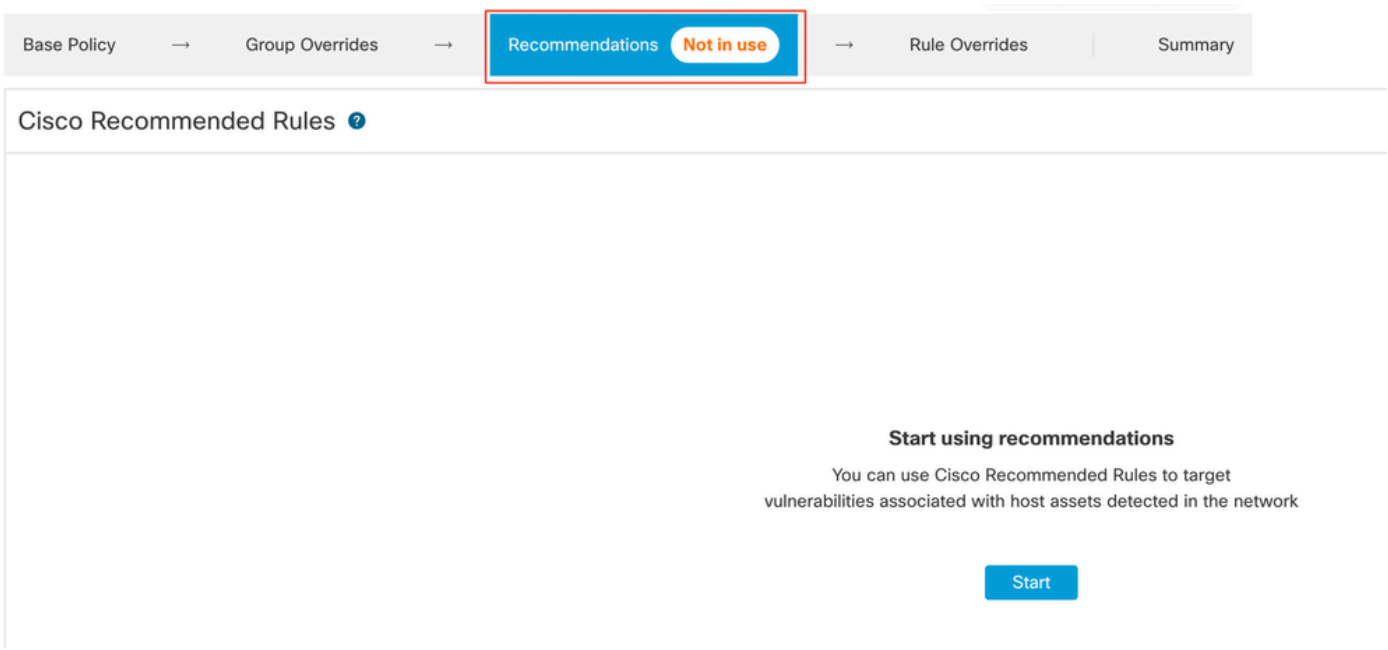
مجموعة الوصول الأولية

14. انقر فوق **View Rules in Rule Overrides**زر لعرض القواعد المختلفة، تفاصيل القاعدة، إجراءات القاعدة، وهكذا للقواعد المختلفة.

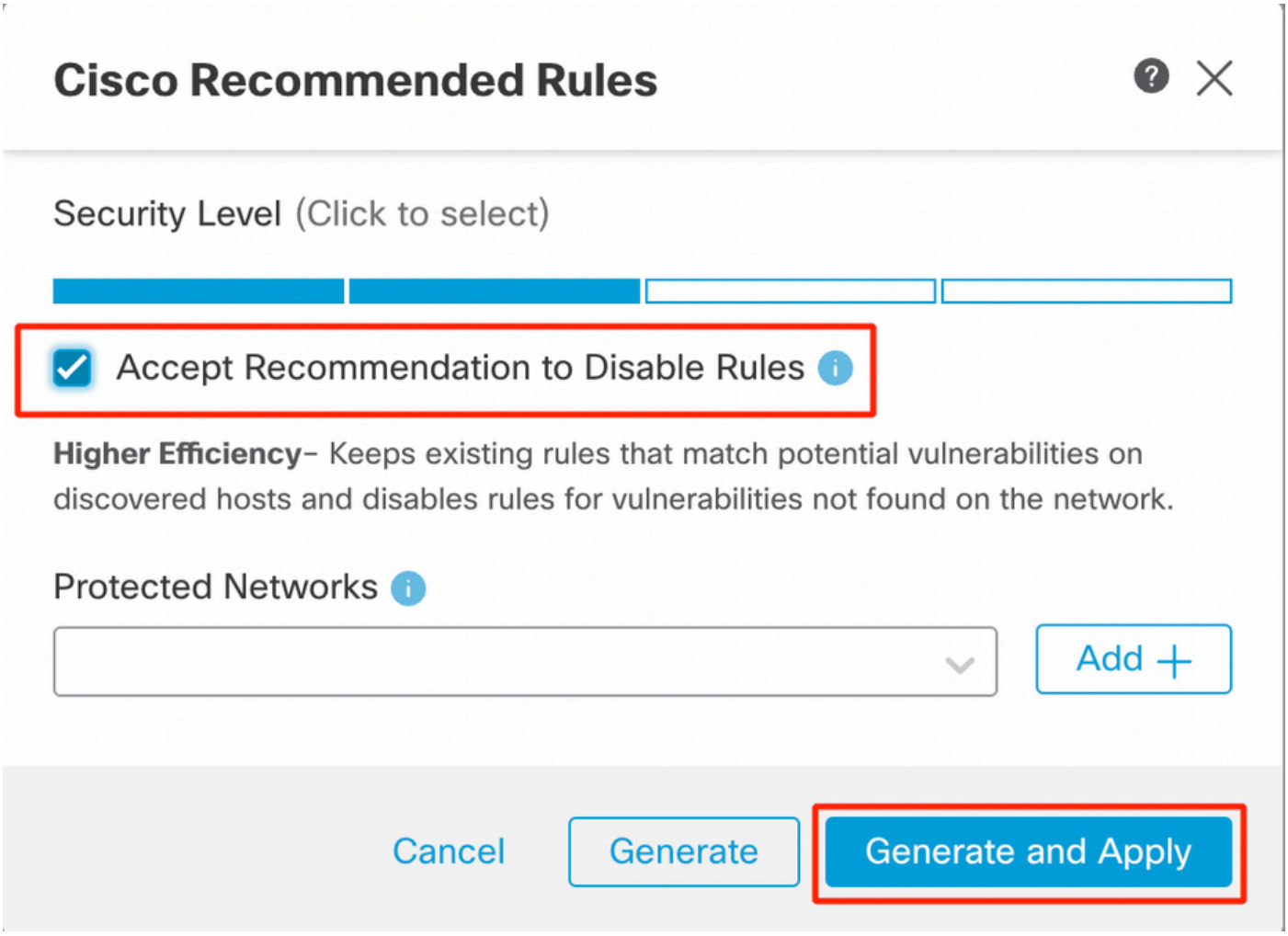


القواعد في تجاوزات القاعدة

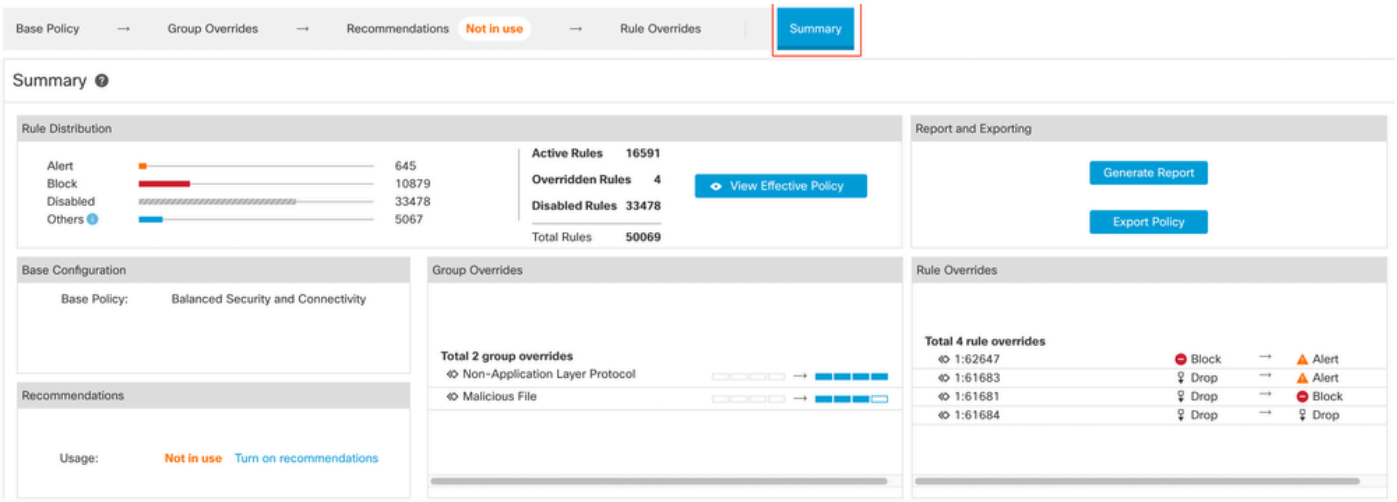
15. انقر فوق Recommendations ثم انقر Start لبدء إستخدام القواعد التي توصي بها Cisco. يمكنك إستخدام توصيات قاعدة التطفل لاستهداف نقاط الضعف المرتبطة بأصول المضيف التي تم الكشف عنها في الشبكة. للحصول على المزيد من المعلومات.



توصيات



16. انقر فوق Summaryطبقة لعرض شامل للتغييرات الحالية على السياسة. يمكنك عرض توزيع قاعدة النهج وتخطيات المجموعة وتخطيات القواعد وما إلى ذلك.



ملخص النهج

عرض أحداث التطفل

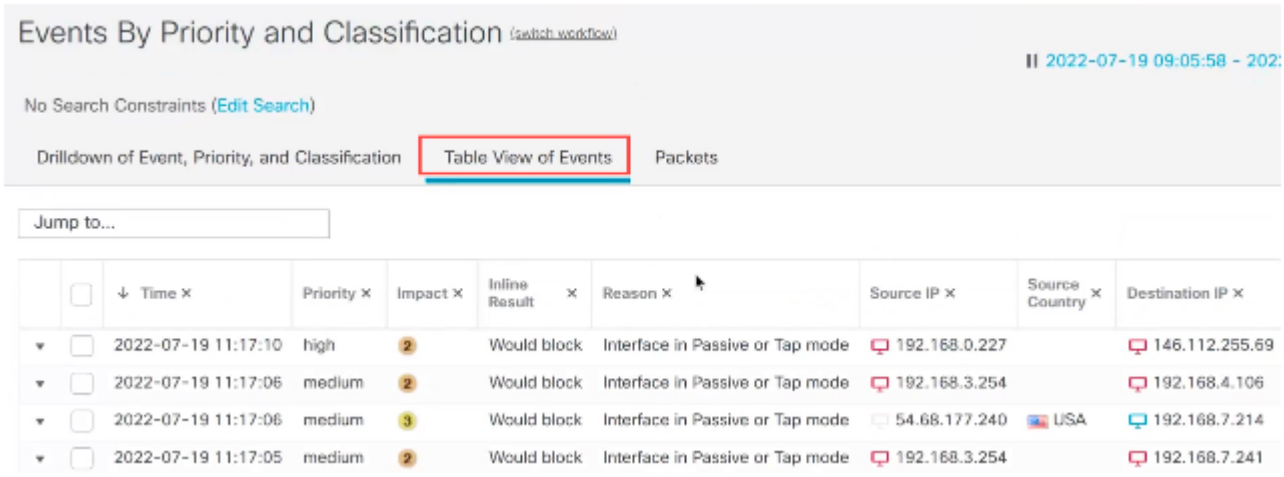
يمكنك عرض تقنيات Miter ATT&CK ومجموعات القواعد في أحداث التطفل في عارض الأحداث الكلاسيكي وعارض الحدث الموحد. يوفر Talos تعيينات من قواعد snort (GID:SID) إلى تقنيات Miter ATT&CK ومجموعات القواعد. يتم تثبيت هذه التعيينات كجزء من حزمة الأمان

في الوضع Lightweight (LSP).

قبل البدء، يجب نشر سياسات التحكم في الوصول والتطفل للكشف عن الأحداث التي تم تشغيلها بواسطة قواعد الشخر وتسجيلها.

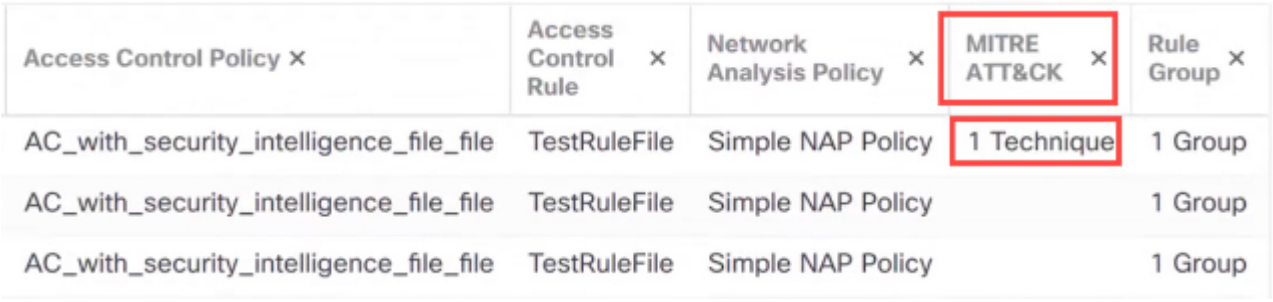
1. انقرAnalysis > Intrusions > Events.

2. انقر فوق **Table View of Events**علامة التبويب كما هو موضح في الصورة.



الأحداث

3 - في MITRE ATT&CKرأس العمود، يمكنك رؤية تقنيات حدث التسلل.

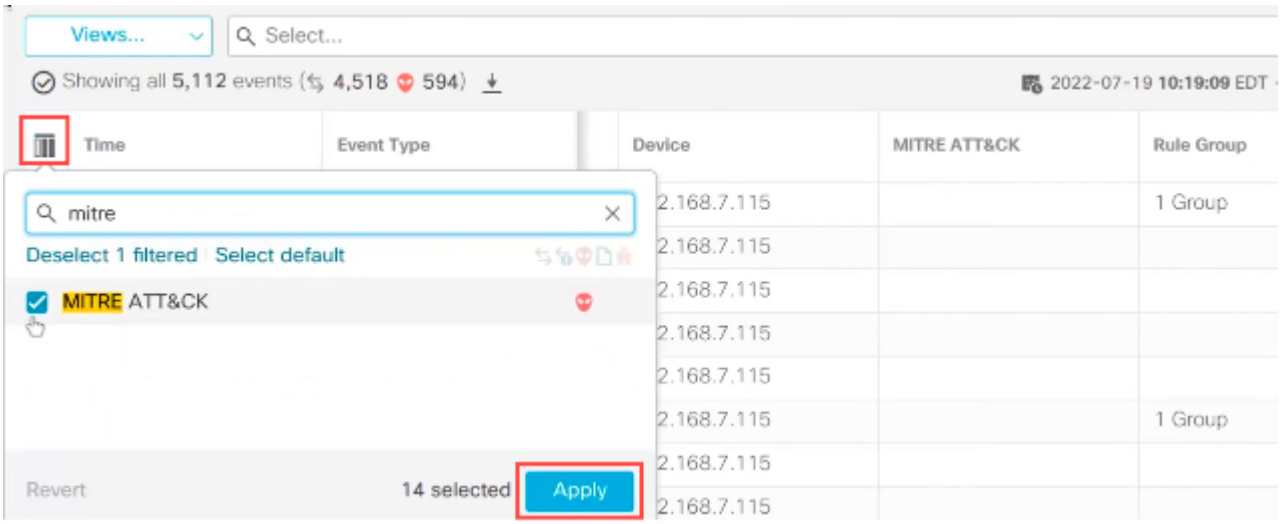


رأس عمود المؤشر

4. انقر 1 Technique(ج) الاطلاع على تقنيات MITER ATT&CK، على النحو المبين في هذا الشكل. في هذا المثال، Exploit Public-Facing Applicationهو التقنية.

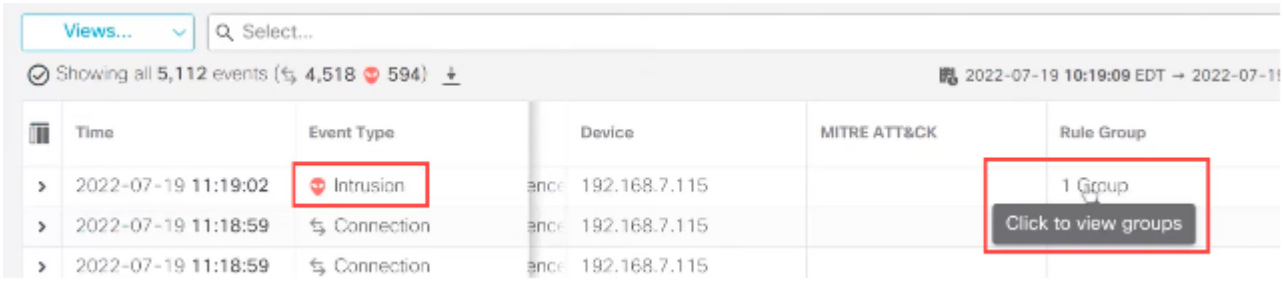
تقنيات Miter ATT&Ck

5. انقرClose.
6. انقرAnalysis > Unified Events.
7. يمكنك النقر فوق رمز محدد العمود لتمكينRule Groupالعموديني وMITRE ATT&CK.



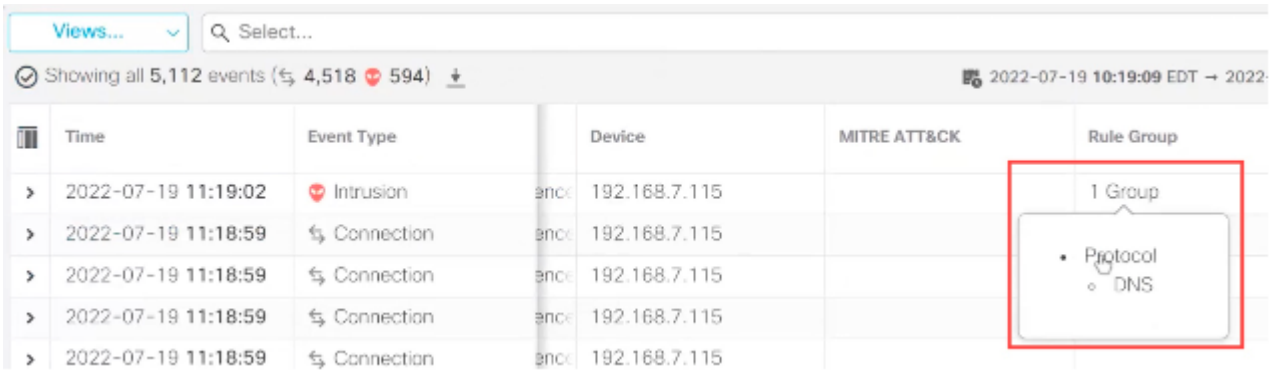
تمكين هجوم الوتر

8. كما هو موضح في المثال هنا، تم إطلاق حدث التسلل من خلال حدث تم تعيينه إلى مجموعة قواعد واحدة. انقر1 Group أسفل Rule Groupعمود.



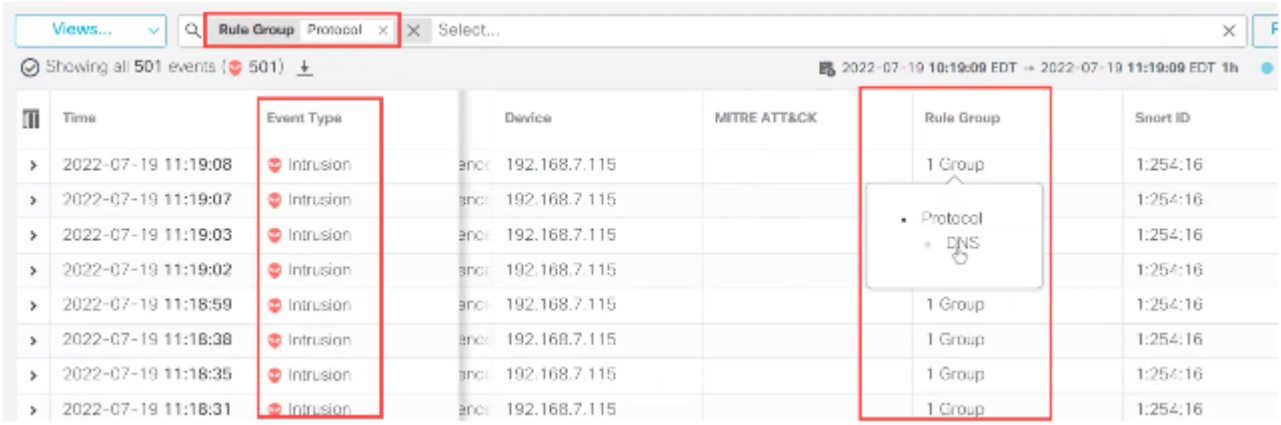
مجموعة القواعد

9. كمثال، يمكنك عرض "البروتوكول"، وهو مجموعة القواعد الأصلية، ومجموعة قواعد DNS الموجودة تحته.



عرض البروتوكول

10. يمكنك النقرProtocolللبحث عن جميع أحداث التطفل التي تحتوي على مجموعة قواعد واحدة على الأقل، وهيProtocol > DNS. يتم عرض نتائج البحث، كما هو موضح في المثال هنا.



بروتوكول مجموعة القواعد

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).