使用MITRE框架查看安全FMC中的潜在威胁并采取相应措施

目录

简介

本文档介绍如何使用MITRE框架查看安全Firepower管理中心(FMC)中的潜在威胁并对其采取行动。

背景信息

MITER ATT&CK(Anagarial Tacustics， Techniques， and Common Knowledge)框架是一个广泛的知识库和方法，提供对威胁发起者针对危害系统发布的战术、技术和程序(TTP)的洞察。ATT&CK被编译成矩阵，每个矩阵代表操作系统或特定平台。攻击的每个阶段（称为“战术”）都对应用于实现这些阶段的特定方法（称为“技术”）。

ATT&CK框架中的每项技术都随附有关技术、相关程序、可能的防御和检测以及实际实例的信息。MITER ATT&CK框架还包含多个组，这些组根据使用的策略和技术集合来指代威胁组、活动组或威胁实施者。通过使用组，框架可帮助对行为进行分类并记录行为。

有关MITRE的详细信息，请参阅https://attack.mitre.org。

先决条件

要求

Cisco 建议您了解以下主题：

- Snort知识
- 安全FMC
- 安全Firepower威胁防御(FTD)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 本文档适用于所有Firepower平台
- 运行软件版本7.3.0的安全FTD
- 运行软件版本7.3.0的安全Firepower管理中心虚拟(FMC)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

MITER框架的优势

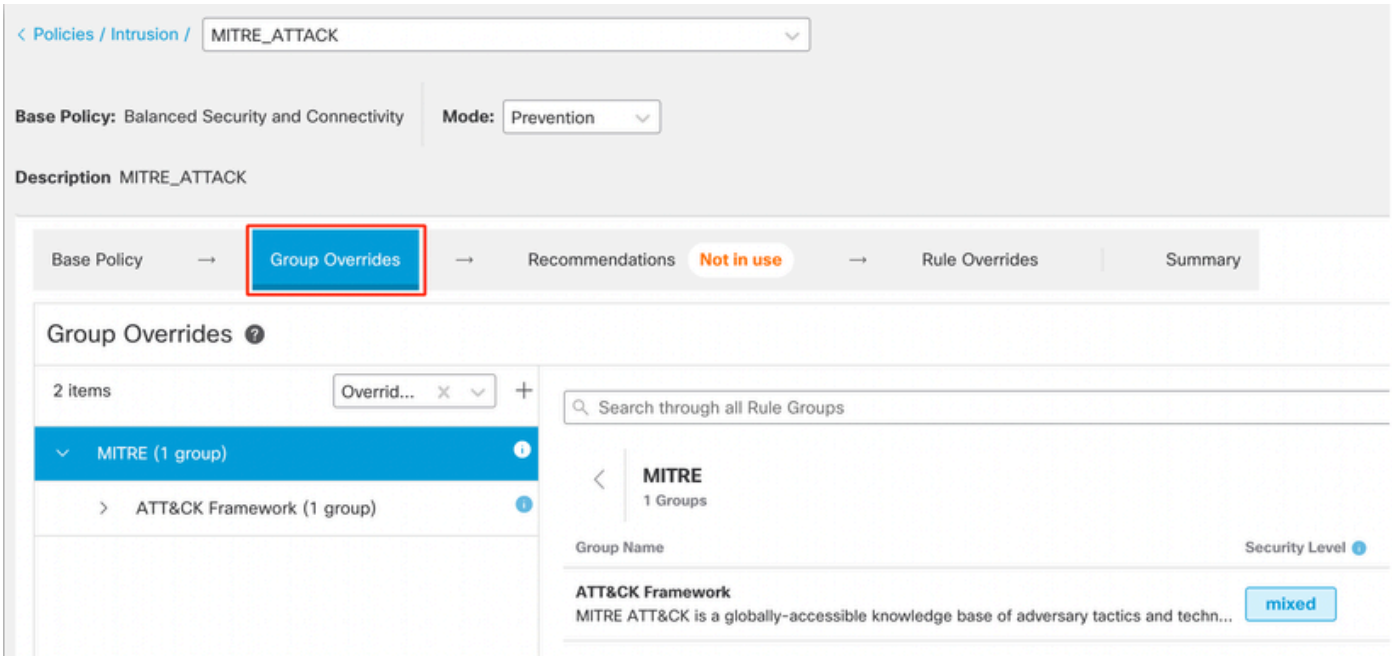
- MITRE策略、技术和过程(TTP)已添加到入侵事件中，使管理员能够根据MITRE ATT&CK(Adversary Tactics Technologies and Common Knowledge)框架对流量执行操作。这使管理员能够更精细地查看和处理流量，并且他们可以根据漏洞类型、目标系统或威胁类别对规则进行分组。
- 您可以根据MITER ATT&CK框架组织入侵规则。这样，您就可以根据特定的攻击者策略和技巧自定义策略。

查看入侵策略中的MITER框架

MITER框架使您能够浏览入侵规则。MITER只是规则组的另一类别，并且是Talos规则组的一部分。支持多个级别规则组的规则导航，为规则提供了更大的灵活性和逻辑分组。

1.选择Policies > Intrusion。
2.确保选中Intrusion Policies该选项卡。
3.单击Snort 3 Version要查看或编辑的入侵策略旁边。关闭弹出的Snort帮助指南。
4.单击Group Overrides层。

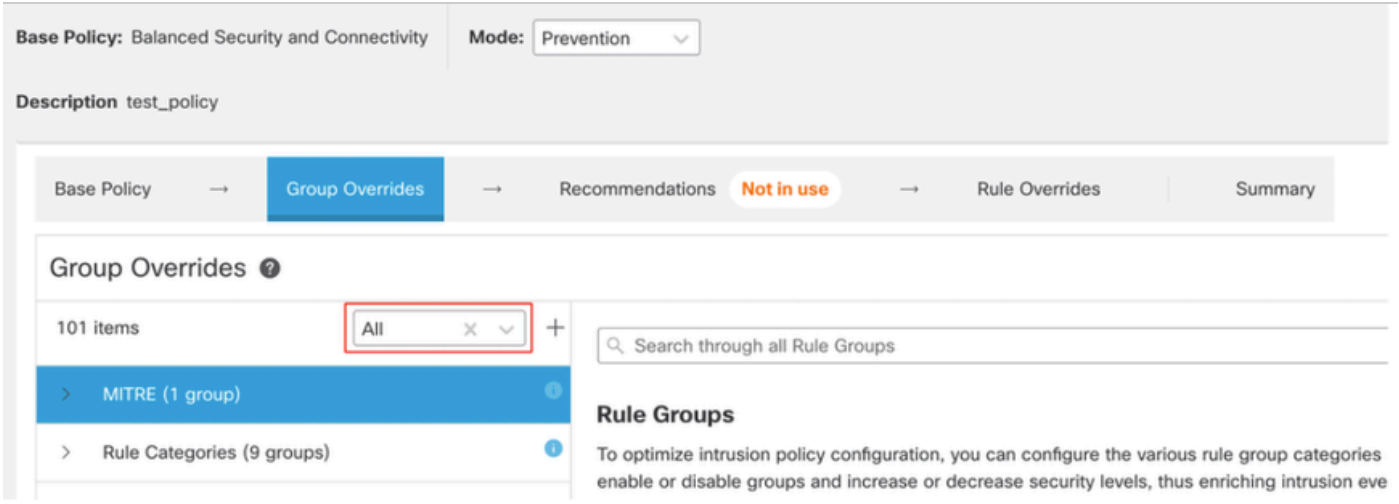
该Group Overrides层在分层结构中列出规则组的所有类别。您可以遍历到每个规则组中的最后一个枝叶规则组。



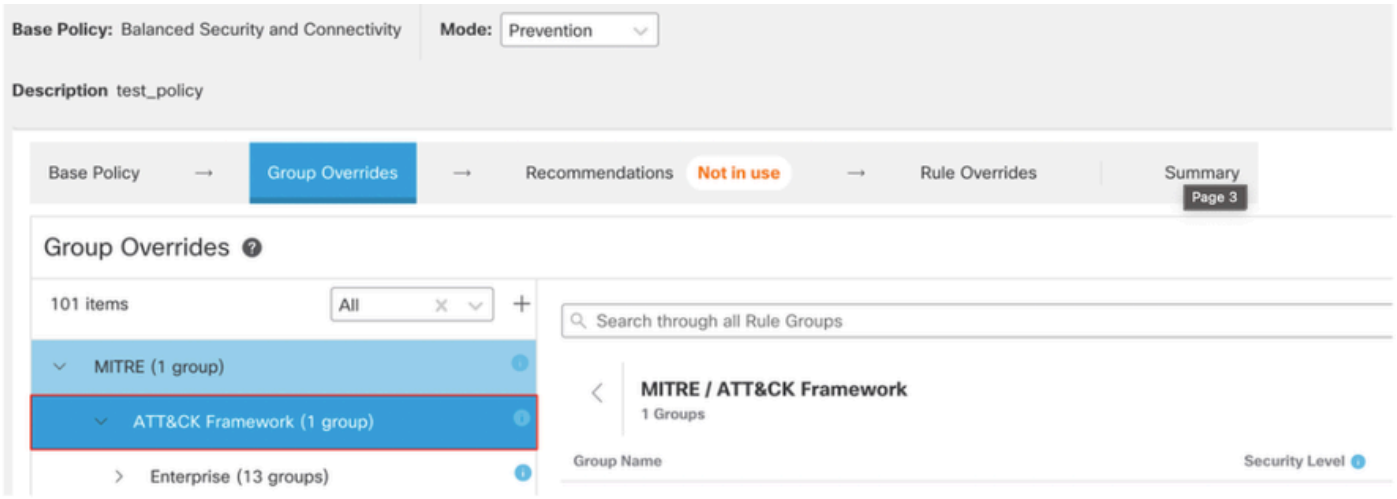
6.在Group Overrides下，确保 All在下拉列表中选择，以便在左侧窗格中看到入侵策略的所有规则组。

7.单击 MITRE在左侧窗格中。

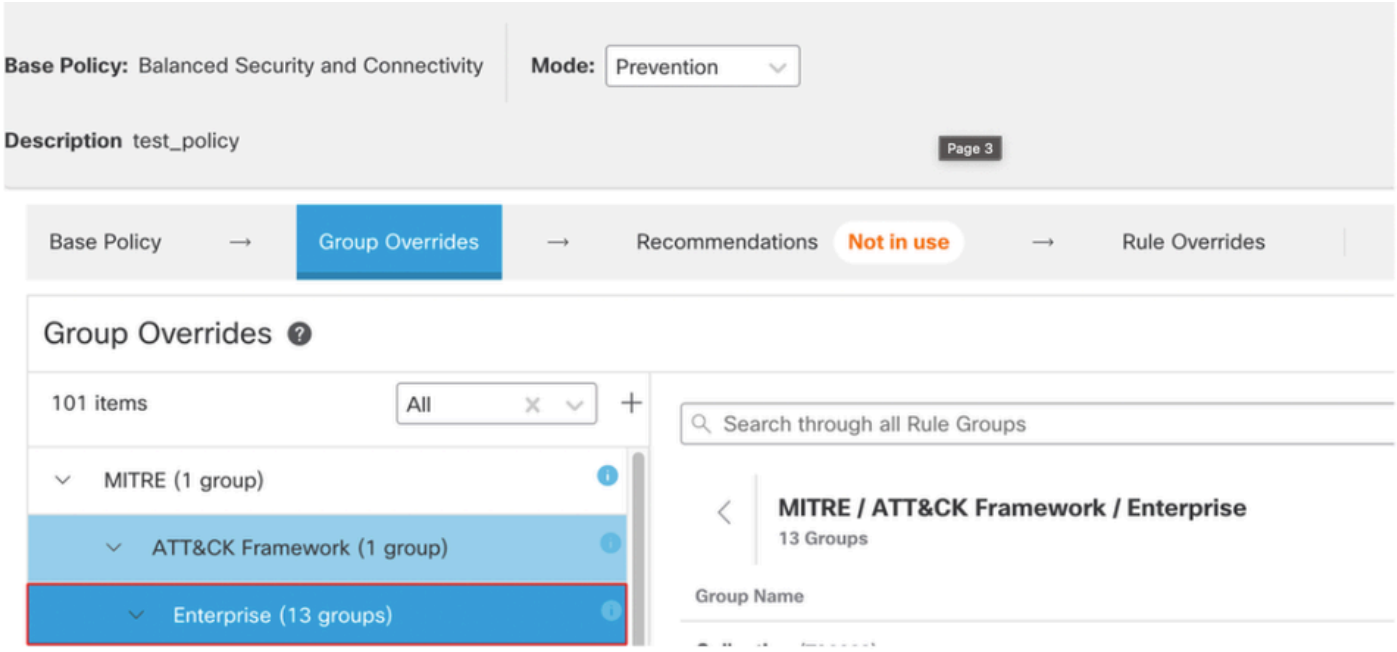
注意：在本示例中，选择了MITER，但根据您的特定要求，您可以选择Rule Categories规则组或规则组下的任何其他规则组和后续规则组。所有规则组都使用MITER框架。



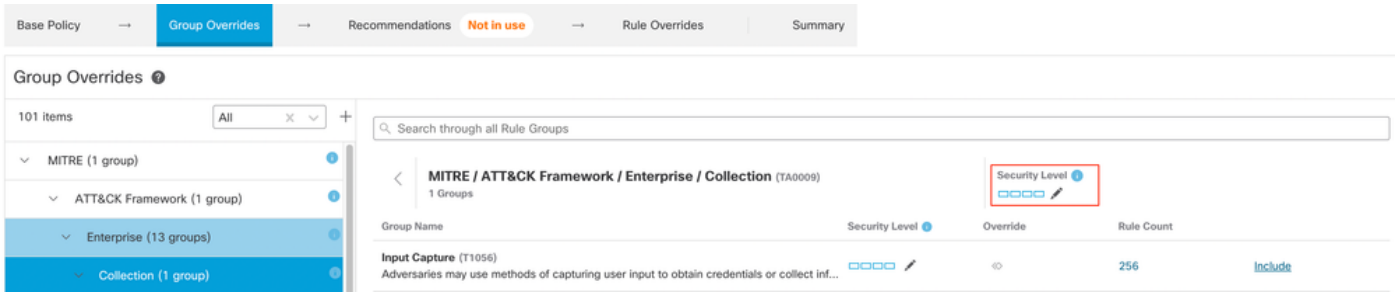
8.在MITRE下，单击ATT&CK“框架”将其展开。



9.在ATT&CK Framework下，单击“企业”将其展开。

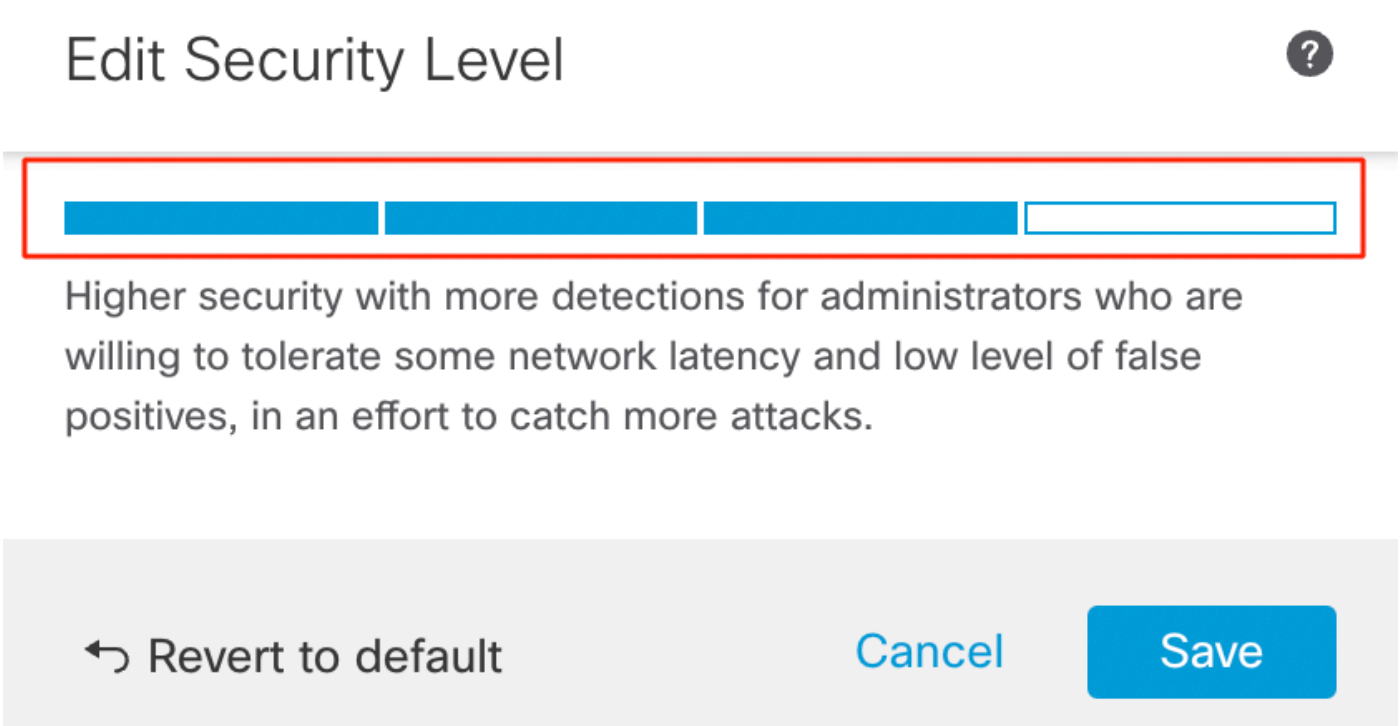


10.单Edit ( ) 击规则组的“安全级别”旁边以对 Enterprise规则组类别。



编辑安全规则组

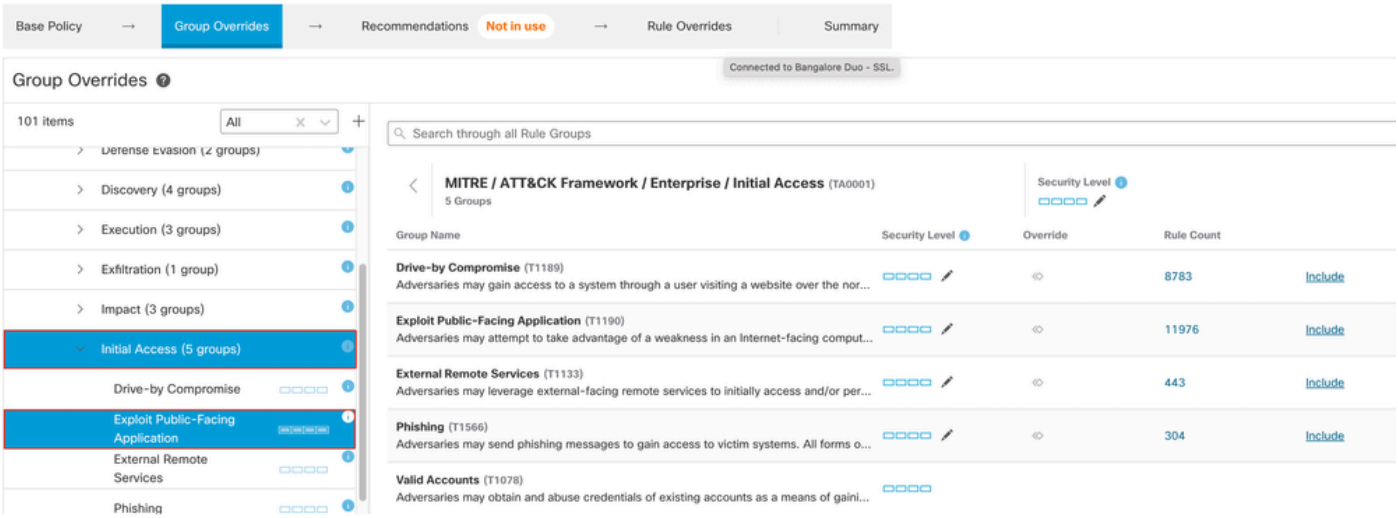
11.例如，在窗口中选择安全级别3Edit Security Level ，然后单击**Save**。



安全级别

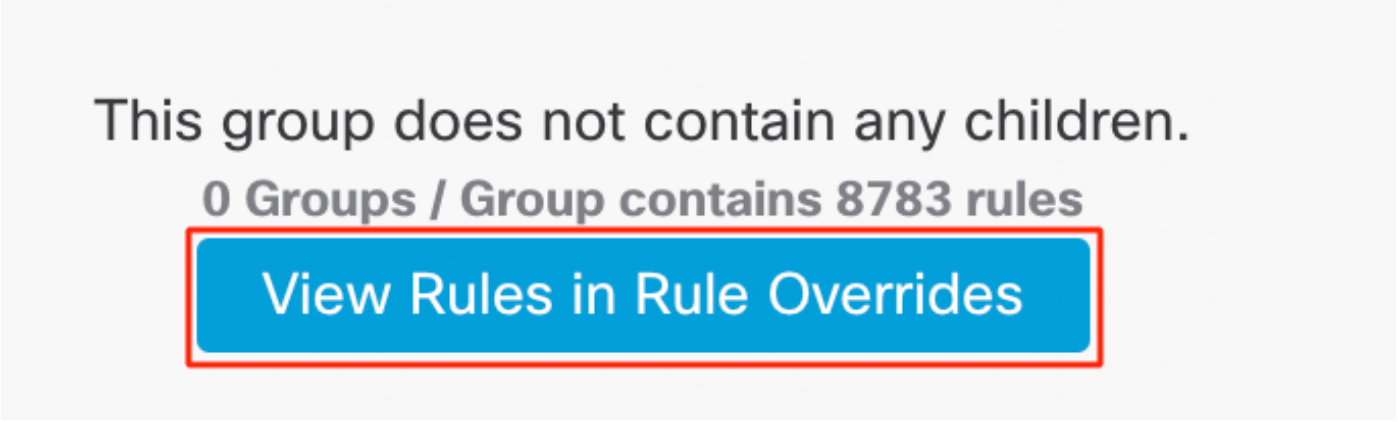
12.在Enterprise下，单Initial Access击将其展开。

13.在Initial Access下，单击Exploit Public-Facing Application，这是最后一个叶组。



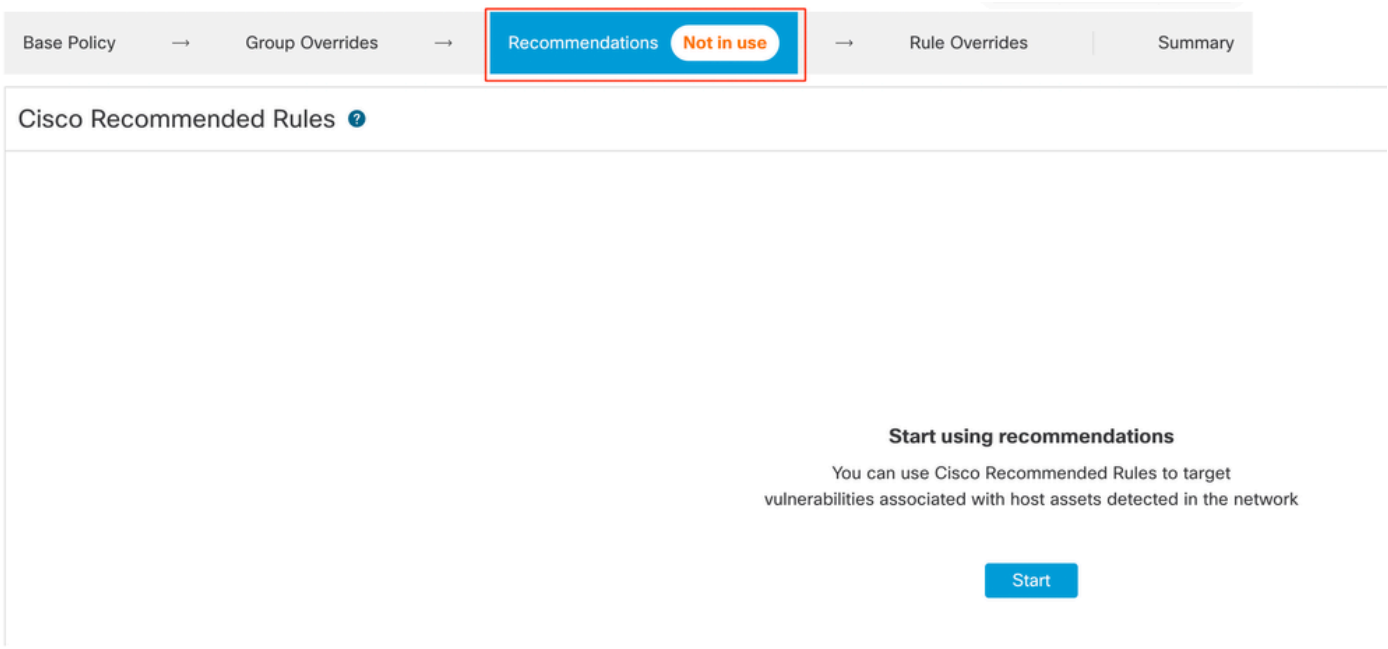
初始访问组

14.单击 **View Rules in Rule Overrides**按钮可查看不同规则的不同规则、规则详细信息、规则操作等。

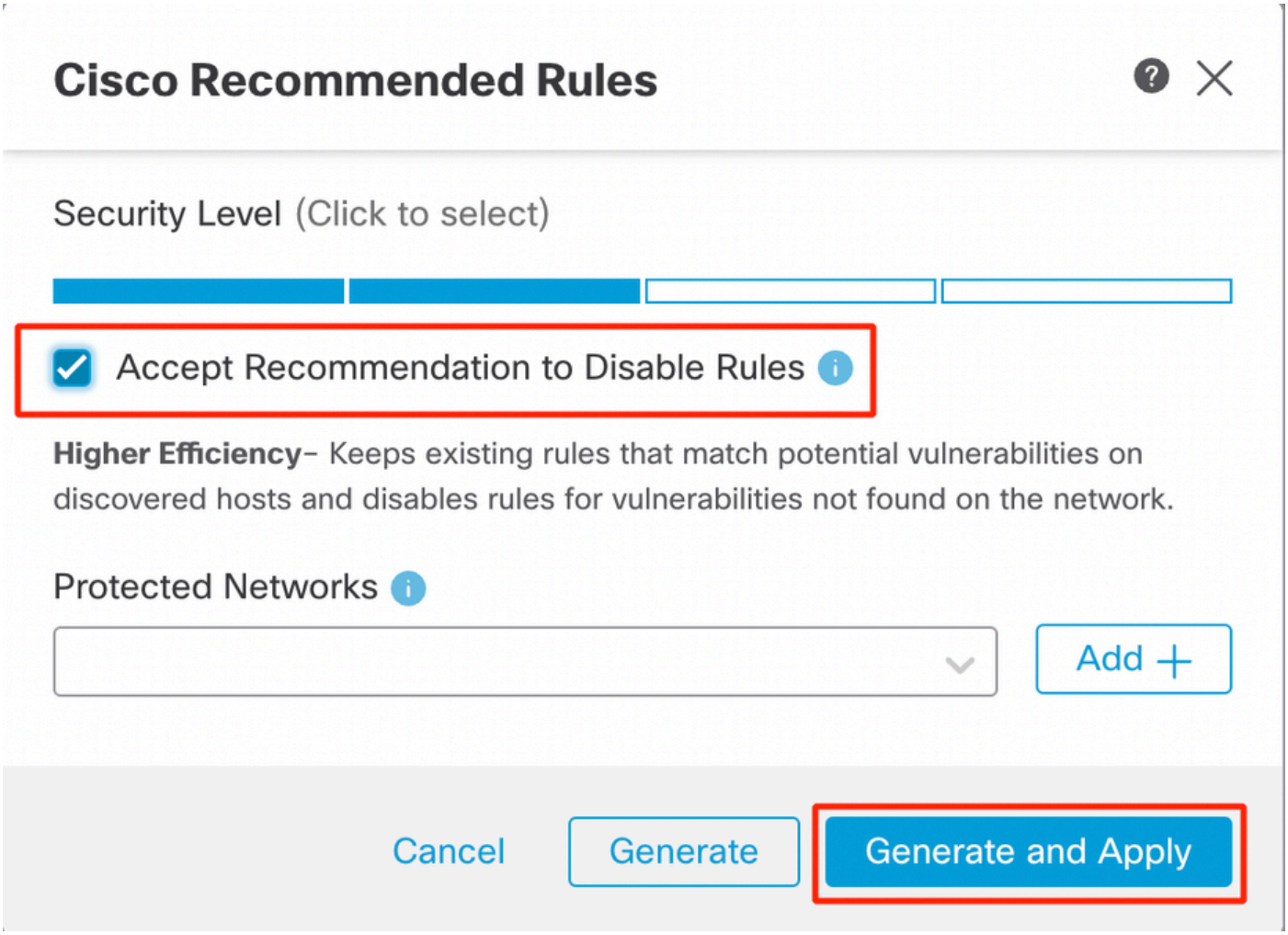


规则覆盖中的规则

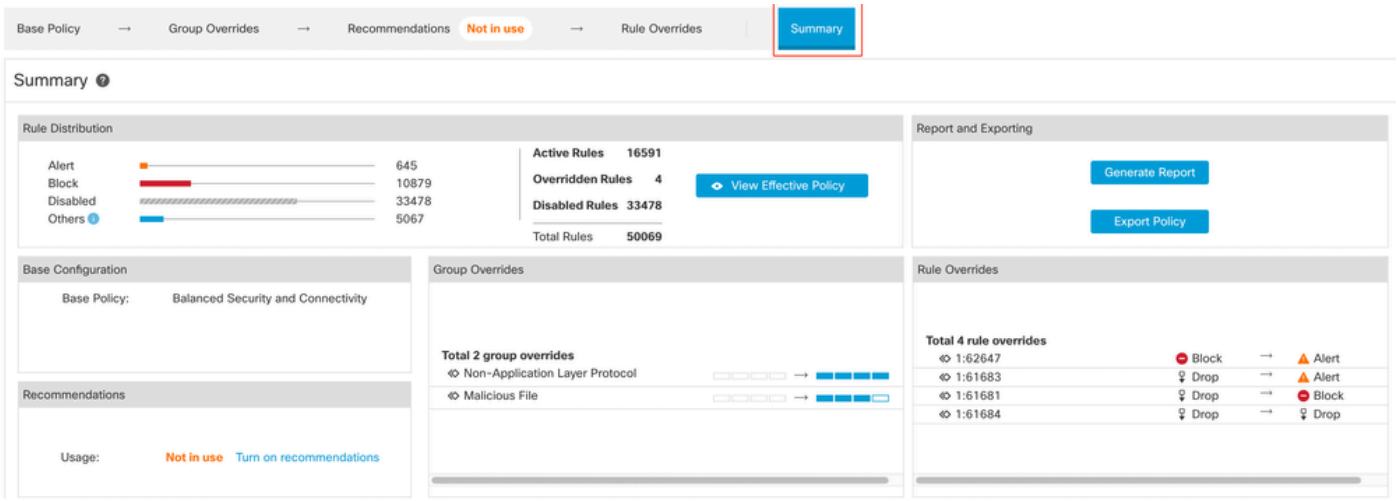
15.单击 Recommendations然后点击Start，开始使用思科推荐的规则。您可以使用入侵规则建议来定位与网络中检测到的主机资产关联的漏洞。有关详细信息.



建议



16.单击 Summary以获取策略当前更改的整体视图。您可以查看策略的规则分布、组覆盖、规则覆盖等。



策略摘要

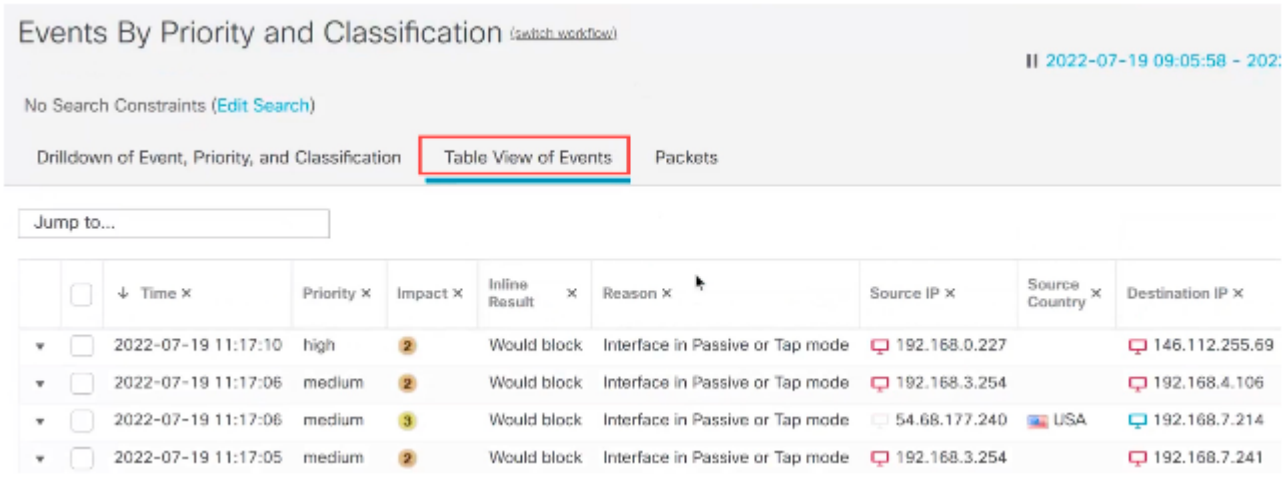
查看入侵事件

您可以在经典事件查看器和统一事件查看器的入侵事件中查看MITER ATT&CK技术和规则组。Talos提供从Snort规则(GID:SID)到MITER ATT&CK技术和规则组的映射。这些映射将作为轻型安全包(LSP)的一部分安装。

开始之前，必须部署入侵和访问控制策略，以检测和记录Snort规则触发的事件。

1.单击Analysis > Intrusions > Events。

2.单击 **Table View of Events**选项卡，如图所示。



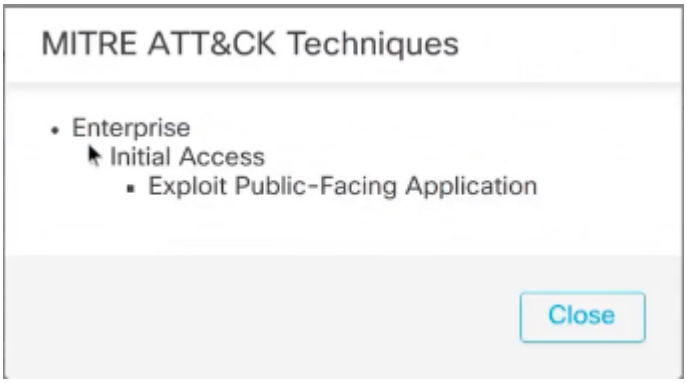
事件

3.在 MITRE ATT&CK列报头，您可以查看入侵事件的技术。

Access Control Policy	Access Control Rule	Network Analysis Policy	MITRE ATT&CK	Rule Group
AC_with_security_intelligence_file_file	TestRuleFile	Simple NAP Policy	1 Technique	1 Group
AC_with_security_intelligence_file_file	TestRuleFile	Simple NAP Policy		1 Group
AC_with_security_intelligence_file_file	TestRuleFile	Simple NAP Policy		1 Group

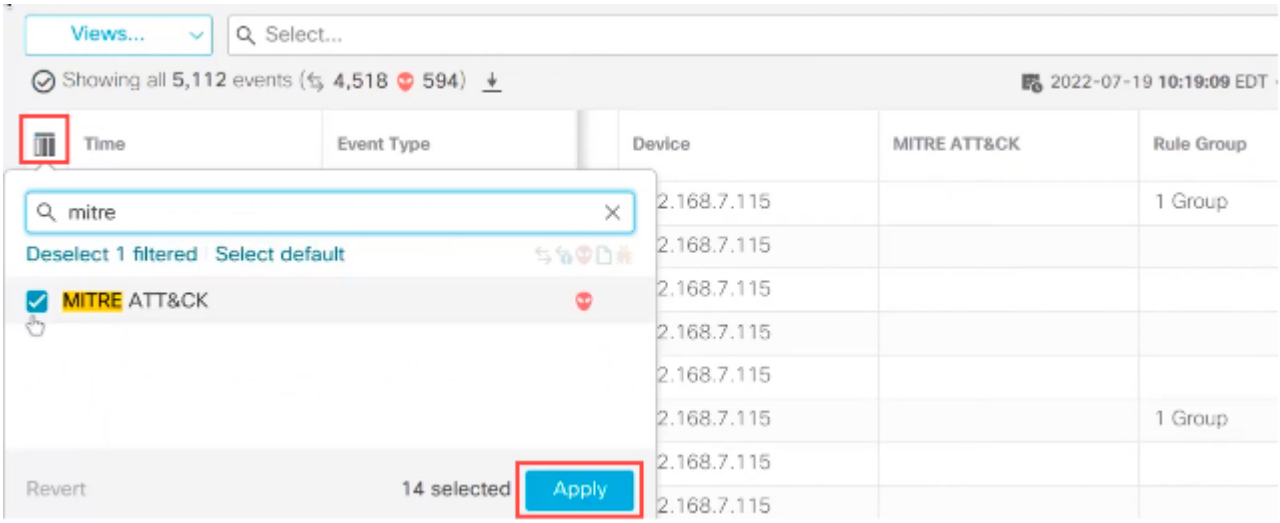
斜接列标题

4.单击 1 Technique查看MITER ATT&CK技术，如图所示。在本例中， Exploit Public-Facing Application就是技术。



MITER ATT&CK技术

5.单击Close。
6.单击Analysis > Unified Events。
7.您可以单击列选择器图标以启用MITRE ATT&CK和Rule Group列。

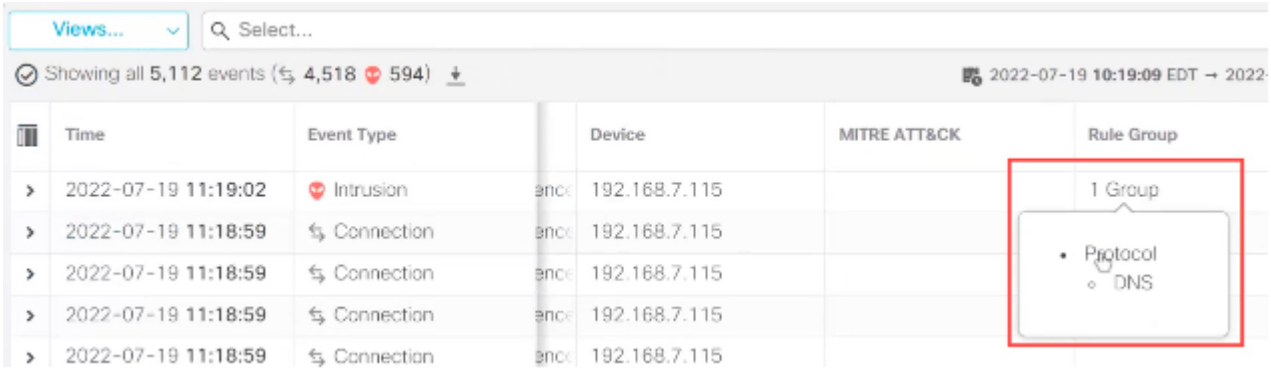


启用Miter攻击

8.如下面的示例所示，入侵事件由映射到某个规则组的事件触发。单1 Group 击 Rule Group列.

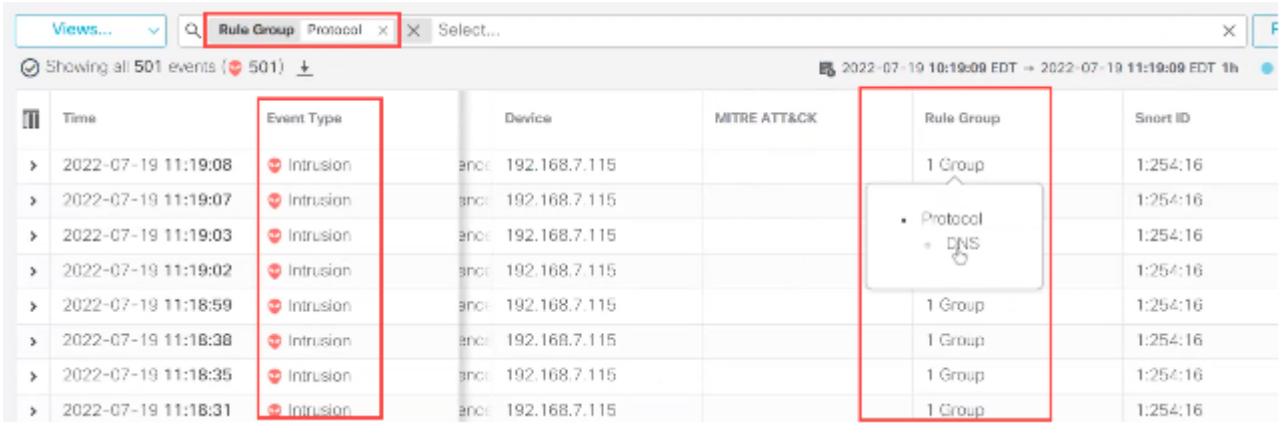
规则组

9.例如，您可以查看协议（父规则组）及其下的DNS规则组。



查看协议

10.可以点击Protocol，搜索至少具有一个规则组的所有入侵事件，即Protocol > DNS。此时将显示搜索结果，如以下示例所示。



规则组协议

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。