在 Snort 3 入侵策略中使用 MITRE 框架缓解威胁

关于 MITRE ATT&CK 框架

MITRE ATT&CK 框架是一个全面的知识库，其中概述了威胁发起者用来破坏系统的战术、技术和程序 (TTP)。它将这些 TTP 组织到不同操作系统和平台的矩阵中，将每个攻击阶段（战术）映射到特定方法（技术）。每种技术都包括有关执行、程序、防御、检测和实际示例的信息。

注释 有关 MITRE ATT&CK 的其他信息，请参阅 https://attack.mitre.org。

管理中心使用 MITRE ATT&CK 框架来增强威胁检测和响应，并纳入以下功能：

- 入侵事件包括 TTP，允许管理员根据漏洞类型、目标系统或威胁类别对规则进行分组，从而更精细地管理流量。
- 选择恶意软件事件使用 TTP，从而增强检测和响应威胁的能力。
- 统一和经典事件查看器显示 Talos 分类中的战术、技术、攻击生命周期图和情景扩充内容。这些扩充内容包括 MITRE 标记以及关联的策略、技术和子技术的分层视图。您还可以使用 MITRE 标识符过滤事件。

MITRE 框架的优势

- MITRE 策略、技术和程序 (TTP) 添加到入侵事件中，使管理员能够根据 MITRE ATT&CK 框架对流量执行操作。这让管理员能够以更精细的方式查看和处理流量，并按漏洞类型、目标系统或威胁类别对规则进行分组。
- 您可以根据 MITRE ATT&CK 框架组织入侵规则。这使您可以根据特定的攻击者战术和技术自定义策略。

MITRE 网络的业务场景示例

一家大型企业网络使用 Snort 3 作为其主要的入侵检测和防御系统。在快速发展的威胁环境中，采用强大的网络安全措施是必要且重要的。网络管理员需要知道配置的策略是否正在查找感兴趣的流量，以及他们是否在跟踪已知的攻击组。例如，您可能想知道攻击者是否试图利用您的系统或应用中的弱点来导致意外行为。系统中的弱点可能是漏洞、故障或设计漏洞。应用可以是网站、数据库、标准服务（例如服务器消息块 (SMB) 或安全外壳 (SSH)）、网络设备管理和管理协议或应用（例如 Web 服务器和相关服务）。

MITRE 框架提供的见解为管理员提供了一个更精确的机会来指定对特定资产的保护并保护其网络免受特定威胁组的侵害。

MITRE 框架的必备条件

- 您必须运行 Cisco Secure Firewall Management Center 和带有 Snort 3 的 Cisco Secure Firewall 威胁防御 7.3.0 或更高版本。
- 必须至少有一个入侵策略。请参阅创建自定义 Snort 3 入侵策略。

查看和编辑 Snort 3 入侵策略

过程

步骤 1 依次选择**策略** > **入侵**。

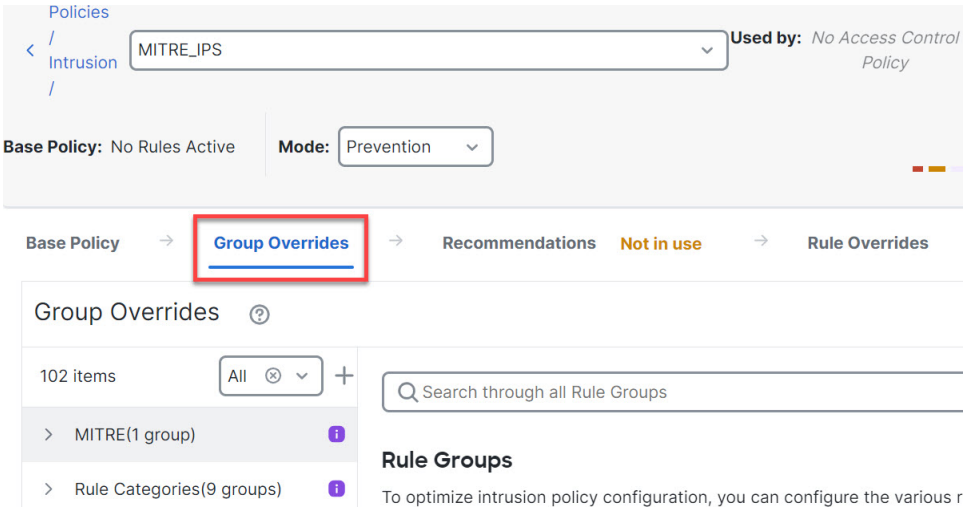
步骤 2 确保选择**入侵策略 (Intrusion Policies)** 选项卡。

步骤 3 点击要查看或编辑的入侵策略旁边的 **Snort 3 版本 (Snort 3 Version)**。

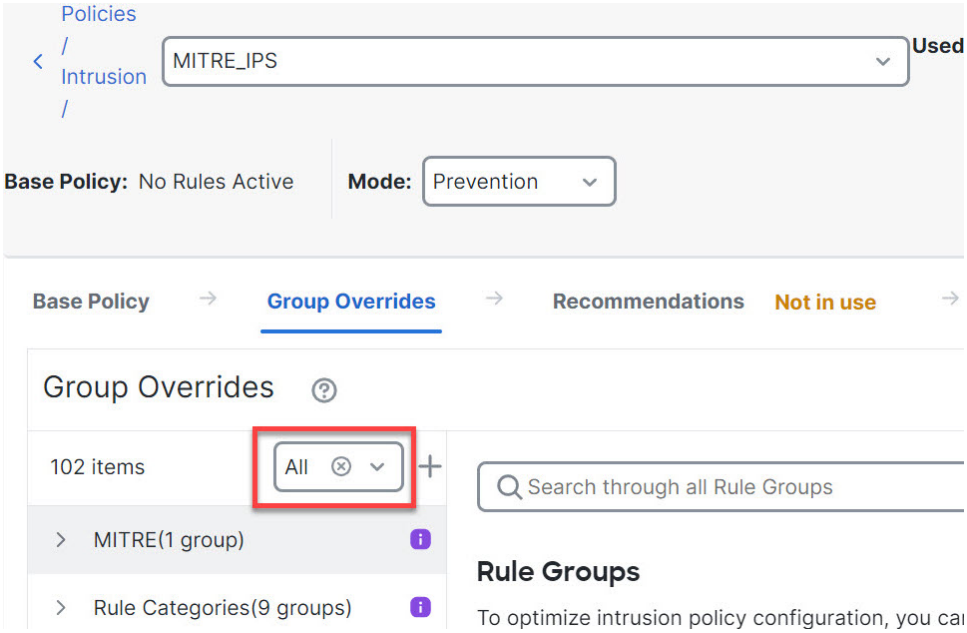
步骤 4 关闭显示的 Snort 助手指南。

步骤 5 点击**组覆盖 (Group Overrides)** 层。

此层以分层结构列出规则组的所有类别。您可以向下展开到每个规则组下的最后一个枝叶规则组。

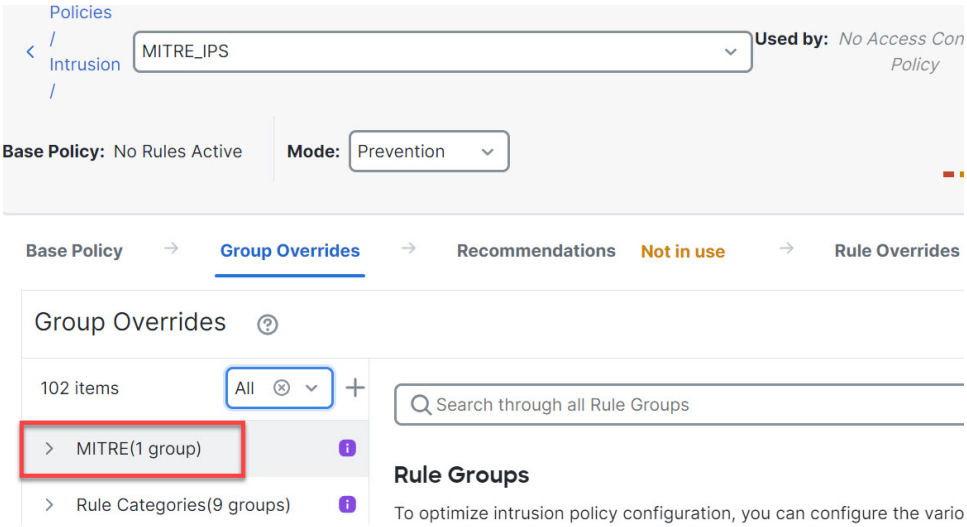


步骤 6 在**组覆盖 (Group Overrides)** 下，确保在下拉列表中选择**全部 (All)**，以便相应入侵策略的所有规则组在左侧窗格中可见。

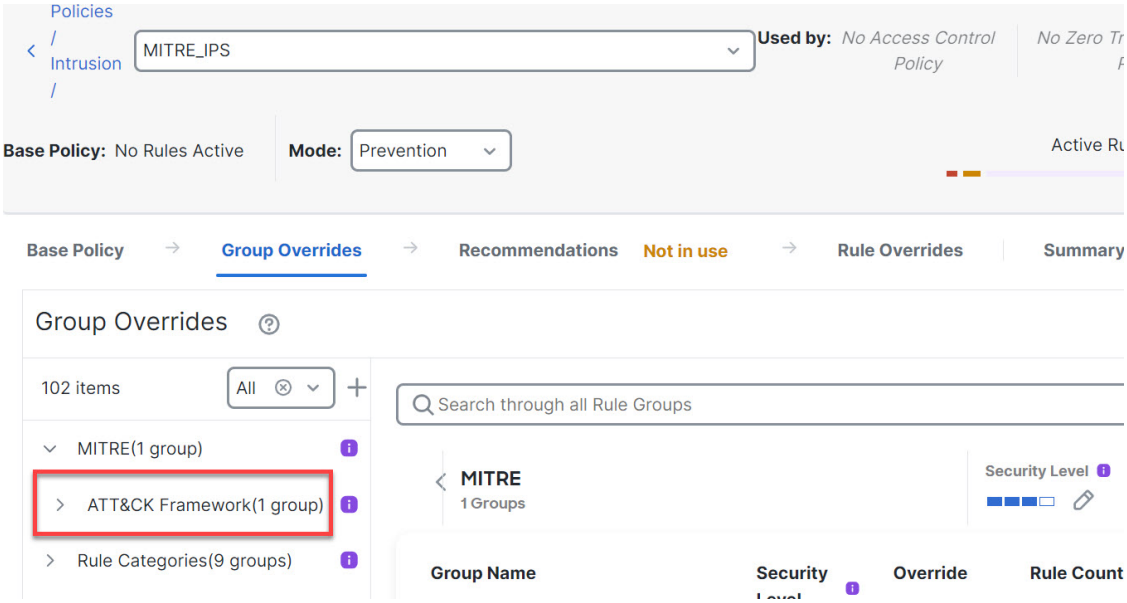


步骤 7 点击左窗格中的 **MITRE**。

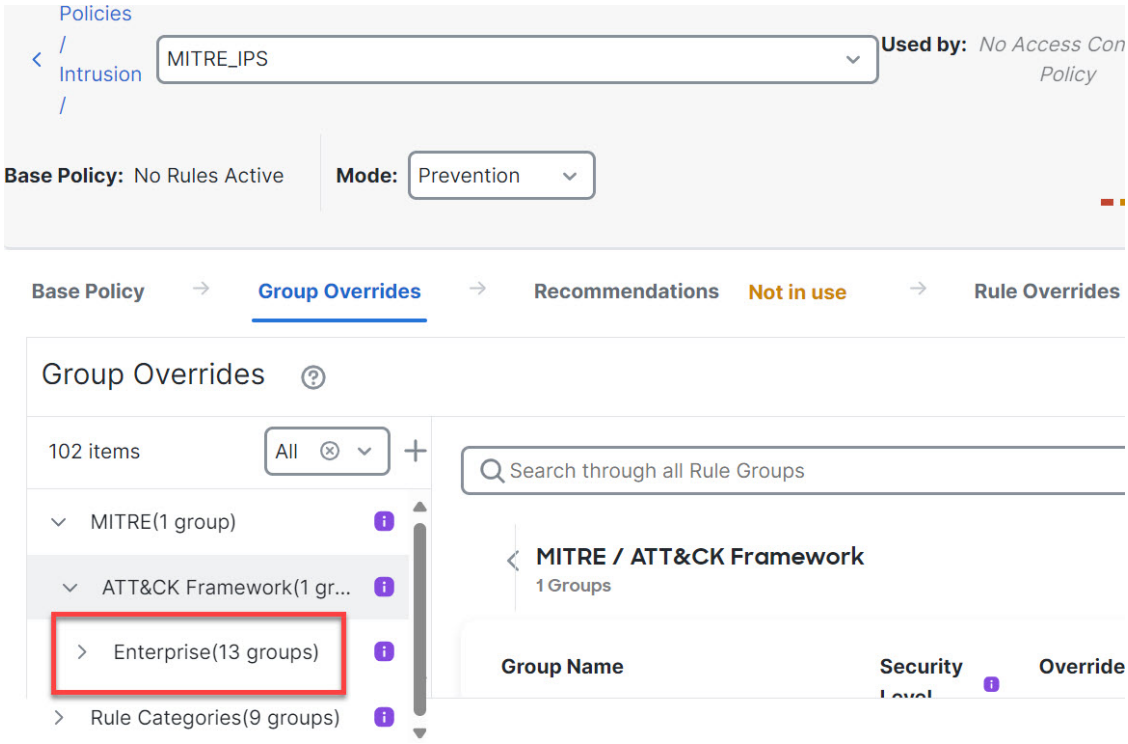
注释
根据您的特定要求，您可以选择**规则类别 (Rule Categories)** 规则组或其下的任何其他规则组和子规则组。所有规则组都使用 MITRE 框架。



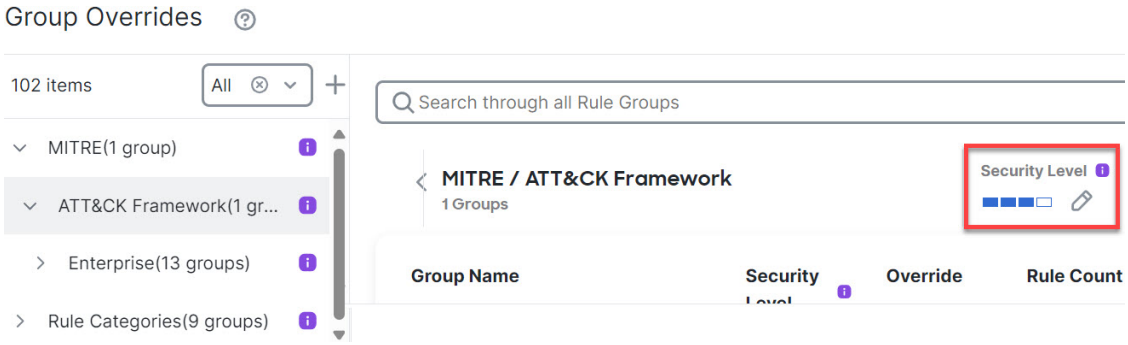
步骤 8 在 **MITRE**下，点击 **ATT&CK 框架 (ATT&CK Framework)** 向下展开。



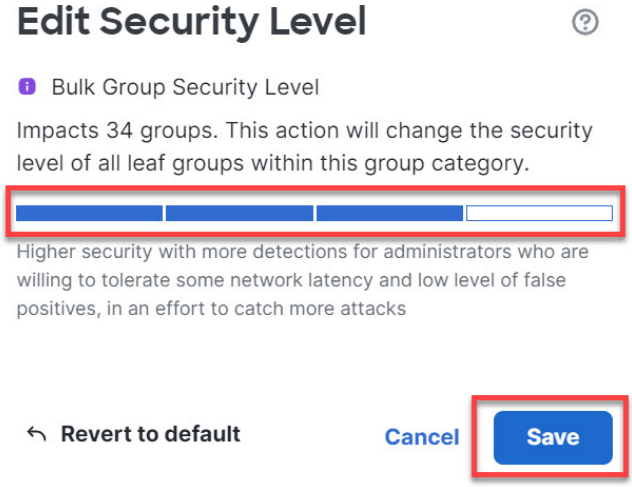
步骤 9 在 **ATT&CK 框架 (ATT&CK Framework)** 下，点击**企业 (Enterprise)** 以将其展开。



步骤 10 点击规则组安全级别 (Security Level) 旁边的 **编辑** (✎) 图标，对**企业 (Enterprise)** 规则组类别下的所有关联规则组的**安全级别**进行批量更改。

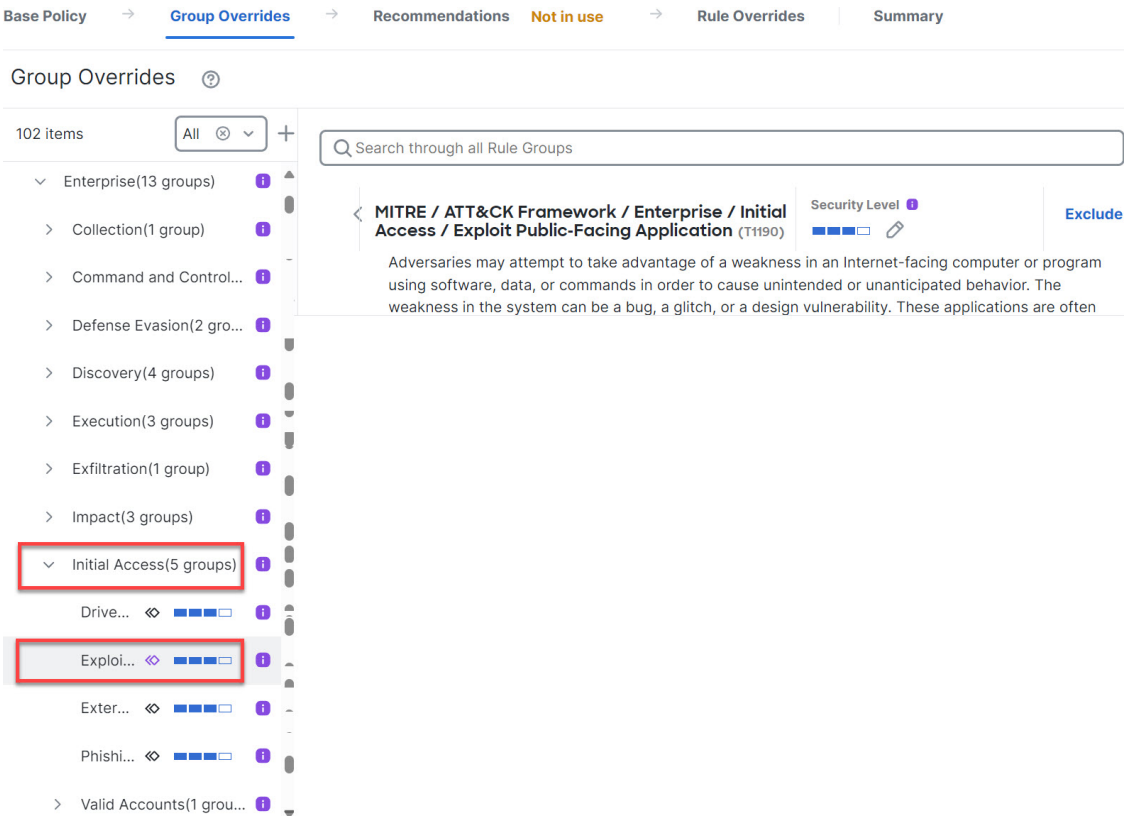


步骤 11 在**编辑安全级别**窗口中，选择**安全级别**（在本例中为 **3**），然后点击**保存**。

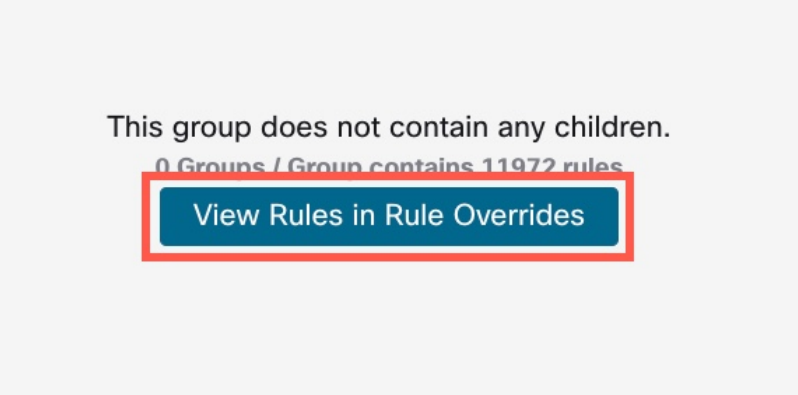


步骤 12 在企业 **(Enterprise)** 下，点击初始访问权限 **(Enterprise)** 将其展开。

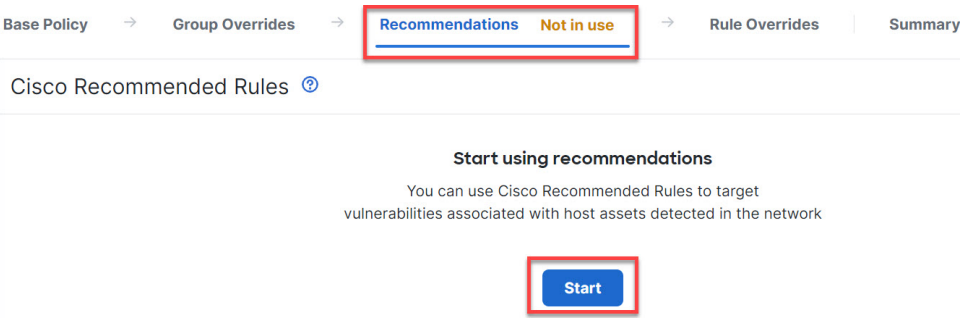
步骤 13 在初始访问权限 **(Initial Access)** 下，点击漏洞攻击面向公众的应用 **(Exploit Public-Facing Application)**，这是最后一个枝叶组。



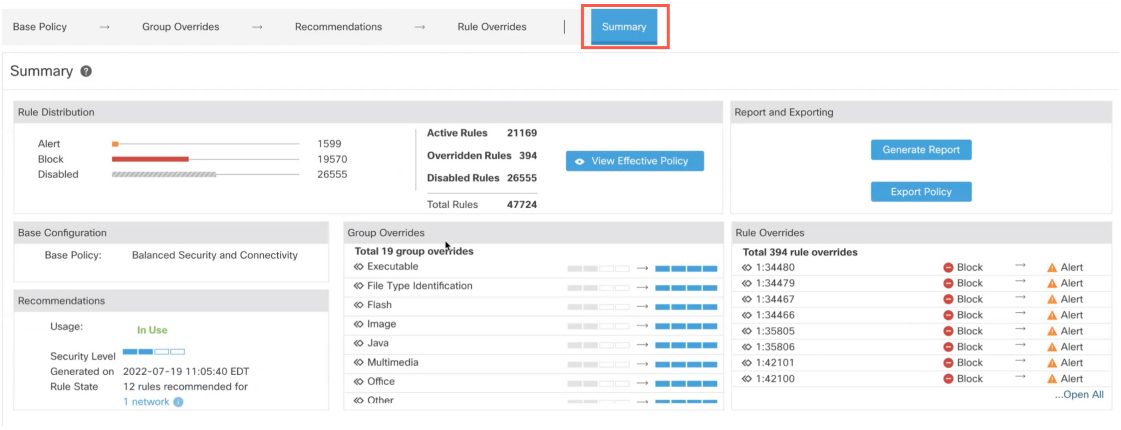
步骤 14 点击查看规则覆盖中的规则 **(View Rules in Rule Overrides)** 以查看不同规则的不同规则、规则详细信息、规则操作等。您可以在规则覆盖 **(Rule Overrides)** 层中更改一个或多个规则的规则操作。



步骤 15 点击**推荐 (Recommendations)** 层，然后点击**开始 (Start)** 以开始使用思科推荐的规则。您可以使用入侵规则建议来锁定与在网络中检测到的主机资产相关联的漏洞。有关详细信息，请参阅在 Snort 3 生成新的 Cisco Secure Firewall 建议。



步骤 16 点击 **摘要** 层可查看当前策略更改的整体视图。根据规则覆盖、安全级别更改和思科推荐规则的生成，您可以查看策略的规则分布、组覆盖、规则覆盖、规则建议等，以验证更改。



下一步做什么

部署入侵策略以检测和记录 Snort 规则触发的事件。请参阅部署配置更改。

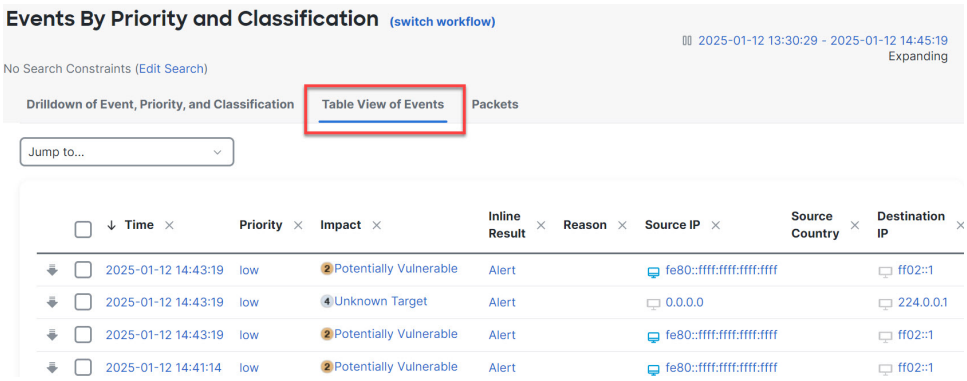
查看入侵事件

您可以在**经典事件查看器 (Classic Event Viewer)** 和**统一事件查看器 (Unified Event Viewer)** 页面上查看入侵事件中的 MITRE ATT&CK 技术和规则组。Talos 提供从 Snort 规则 (GID:SID) 到 MITRE ATT&CK 技术和规则组的映射。这些映射作为轻量级安全软件包 (LSP) 的一部分安装。

过程

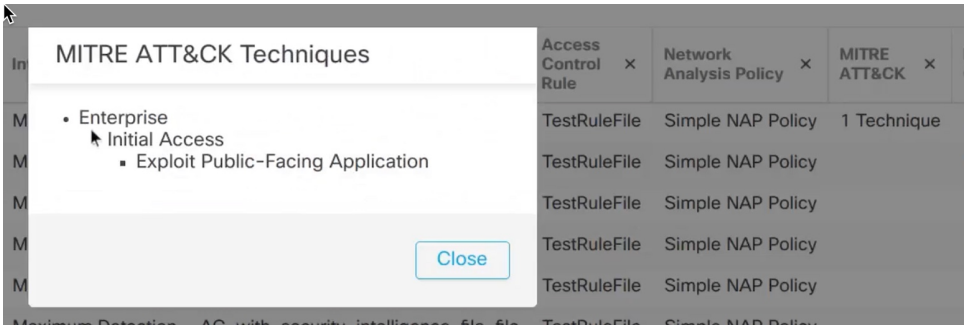
步骤 1 点击**分析 (Analysis)**，然后选择**入侵 (Intrusions)** 下的**事件 (Events)**。

步骤 2 点击**事件的表视图 (Table View of Events)** 选项卡。



步骤 3 在 **MITRE ATT&CK**下，您可以看到入侵事件的技术。点击 **1 技术 (1 Technique)** 以查看 MITRE ATT&CK 技术。

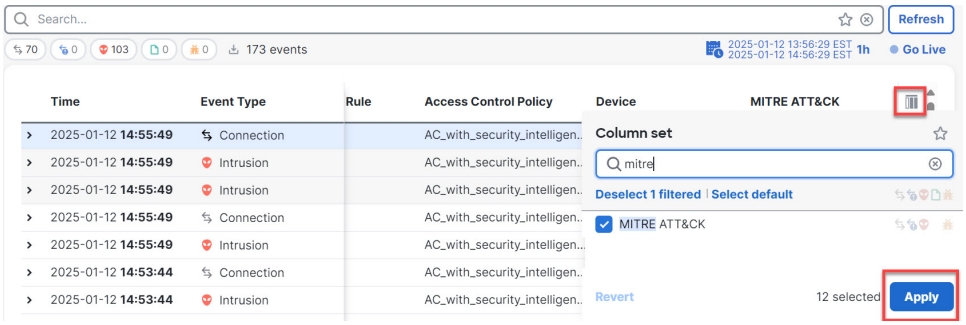
在本例中，攻击技术是**面向公众的应用 (Exploit Public-Facing Application)**。



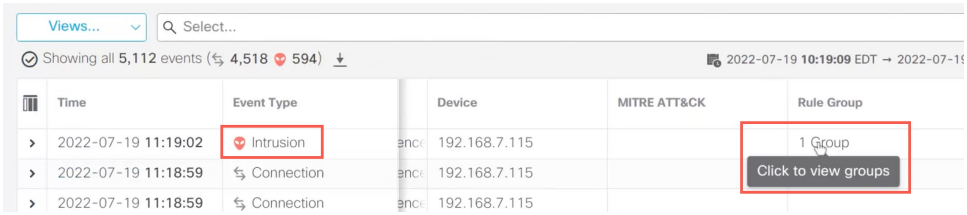
步骤 4 点击**关闭 (Close)**。

步骤 5 点击**分析 (Analysis)**，然后选择**统一事件 (Unified Events)**。

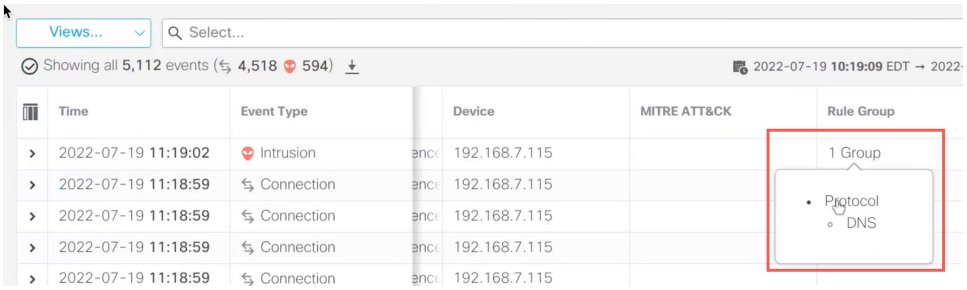
步骤 6 如果未启用，请点击列选择器图标以启用 **MITRE ATT&CK** 和**规则组 (Rule Group)** 列。



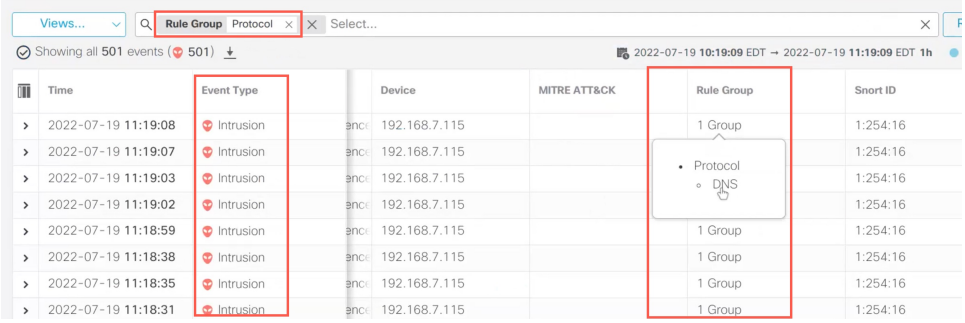
步骤 7 在本示例中，入侵事件由映射到一个规则组的事件触发。点击**规则组 (Rule Group)** 列下的 **1 组 (1 Group)**。



步骤 8 您可以查看**协议 (Protocol)**（父规则组）及其下的 DNS 规则组。选择**协议 (Protocol)** > **DNS** 以搜索具有至少一个规则组的所有入侵事件。



屏幕上会显示搜索结果。



其他参考资料

- Snort 3 中的入侵策略
- 编辑 Snort 3 入侵策略
- 恶意软件事件中的 MITRE 信息

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。