使用Umbrella检查或争议IPS误报

目录

简介

先决条件

- 要求
- 使用的组件

概述

查看IPS检测

协议违规

应用程序兼容性

禁用IPS签名

支持

- 历史事件
- IPS问题/误报

简介

本文档介绍如何使用Cisco Umbrella审核或争议入侵防御服务(IPS)误报。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于Cisco Umbrella。

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。

概述

Cisco Umbrella的入侵防御系统检测（或阻塞）被视为与已知威胁、漏洞相关的数据包，而且只需在数据包的格式不正常时进行检测。

管理员根据以下默认列表选择用于检测威胁的IPS签名列表：

- 连接胜过安全
- 平衡的安全性和连接性

- 安全性高于连接
- 最大检测

请务必记住，选择的签名列表会严重影响遇到的IPS误报数量。最安全的模式（例如最大检测和连接安全性）将创建不必要的IPS检测，因为它们侧重于安全性。只有在需要总体安全性时，才建议使用最安全的模式，并且管理员必须预测监控和查看大量IPS事件的需求。

有关不同模式的详细信息，请参阅IPS文档。

查看IPS检测

使用Umbrella Dashboard上的Activity Search查看IPS事件。对于每个事件，有两个重要信息：

- IPS特征码ID/类别/名称。可在https://snort.org上搜索
- CVE编号（如果适用）。 可在https://www.cve.org/上搜索

并非所有IPS检测都表明存在已知漏洞/攻击。许多签名（特别是在最大检测模式下）只是表示存在特定类型的流量或协议违规。请务必查看前面提到的信息来源以及有关事件的其他详细信息（如源/目标），以确定事件是否需要您的安全团队进行进一步调查。

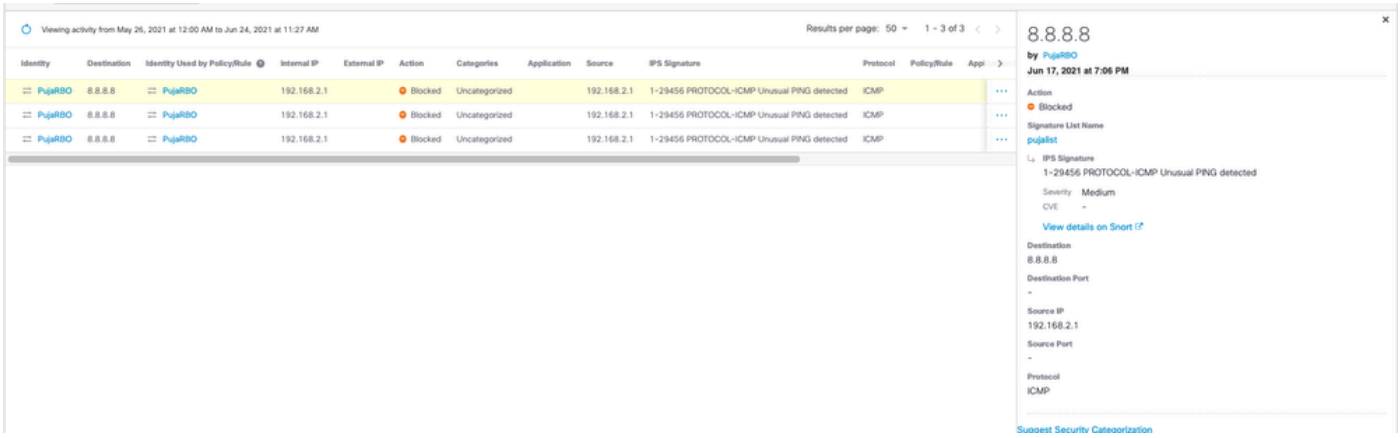
签名类别可用于提供有关IPS检测类型的其他上下文。查看snort.org上提供的类别。

协议违规

在本示例中，IPS事件链接到此签名：
https://www.snort.org/rule_docs/1-29456

签名的说明如下：

“规则会查找进入网络但不遵循PING正常格式的PING流量。”



4403885889428

在这种情况下，Snort规则并不一定检测到任何特定漏洞，而是检测到被阻止的格式错误的ICMP数据包。根据snort.org上提供的信息以及有关该事件的其他详细信息（如源/目标），管理员可以确定无需进一步调查此事件

应用程序兼容性

某些合法应用与IPS签名不兼容，尤其是在配置了更主动（最大检测）模式时。在这些情况下，可以出于协议违规(Protocol Violation)部分中讨论的原因阻止应用。应用可以采用意外方式使用协议，或者通过通常为其他流量保留的端口使用自定义协议。

即使应用是合法的，这些检测通常也是有效的，思科无法始终予以纠正。

如果合法应用被IPS阻止，Umbrella建议联系应用供应商，提供事件/特征码的详细信息。必须测试第三方应用程序与snort.org上的IPS签名的兼容性。

当前无法从IPS扫描中排除单个应用/目标。

禁用IPS签名

如果发现签名导致与第三方应用程序的兼容性问题，则可以禁用签名（临时或永久）。 只有在您信任该应用程序，并且您确定该应用程序的价值超过了特定签名的安全性优势时，才能执行此操作。

有关创建自定义签名列表的信息，请完成添加自定义签名列表文档中的步骤。您可以将当前设置用作模板，然后通过将其设置为Log Only或Ignore来禁用所需的规则。

支持

历史事件

Umbrella支持无法提供有关历史IPS事件的其他详细信息。IPS事件通知您流量与IPS签名不匹配。有关签名的详细信息，请访问snort.org。Umbrella不存储原始流量/数据包的副本，因此无法提供有关IPS事件性质的进一步上下文或确认。

IPS问题/误报

如果您希望对当前的IPS问题（例如误报）提出异议，请与Umbrella支持部门联系。

为了调查这些问题，Umbrella Support需要捕获数据包。需要数据包的原始内容来确定流量如何触发IPS检测。您必须能够复制问题，才能生成数据包捕获。

在生成通知单之前，请在复制问题时使用Wireshark等工具生成数据包捕获。 说明可在我们的知识库中找到。

或者，Umbrella支持可以协助生成数据包捕获。他们需要安排时间，以便重新创建受影响用户或应用程序的问题。

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）。