安全访问活动搜索显示未知的规则名称

目录

问题

在Umbrella到SSE迁移期间，安全访问活动搜索事件将规则名称显示为UNKNOWN，而不是显示命名策略规则。针对各种流量类型观察到此行为，包括允许的流量（例如对chatgpt.com的请求）。问题是这些UNKNOWN规则名称条目是否表示需要补救的策略配置问题或迁移问题。

环境

- 思科安全访问(SSE)
- 正在从Umbrella迁移到SSE的组织
- 安全访问活动搜索报告
- 分类为新发现的域的流量

分辨率

Rule Name UNKNOWN行为对于Secure Access系统逻辑处理的事件（而不是客户创建/命名的规则）是正常行为。这种情况通常发生在分类为新发现的域的流量中，该域在查询时新发现，并在“活动搜索”或“安全活动”报告中报告。

使用未知规则名称解释活动搜索事件

遇到Rule Name UNKNOWN事件时，请查看以下事件字段以确定实施原因并确认正确的策略应用：

- Action — 显示是允许还是阻止流量
- 事件阻止原因/阻止原因 — 提供具体的实施详细信息
- 类别 — 显示内容分类（例如新显示的域）
- 目标域/IP — 请求的目标
- 用户/源身份 — 流量的源
- 时间戳 — 事件发生时间

如果Categories字段显示Newly Seen Domains，则rule-name字段中的UNKNOWN是预期行为，并不表示迁移失败或策略损坏。

意外行为的验证步骤

如果预期流量与特定命名规则匹配，但显示UNKNOWN，请收集此信息以进行策略路径验证：

- 2-3个示例事件时间戳
- 每个事件的目标域/IP
- 每个事件的用户/源身份

此信息可用于比较预期策略路径与实际事件行为，并确定是否需要进一步调查。

原因

当Secure Access系统逻辑处理流量而不是应用客户创建/命名的策略规则时，会显示UNKNOWN规则名称。这是某些流量类别（尤其是新发现的域）的已编档行为，其中内置分类和处理机制在初始域评估期间优先于命名规则。

相关内容

- 启用新显示的域安全

- 思科技术支持和下载

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）。