Cisco XDR已知问题

目录

简介

本文记录当前已知的Cisco XDR技术问题。

技术问题可由思科确认、正在审核、待解决或视为按预期工作。

已知问题：

事件

此XDR功能目前没有已知问题。

调查

此XDR功能目前没有已知问题。

控制中心

1. — 控制中心上的MTTR图块显示已使用一种新状态(例如“已关闭：误报”、“已关闭：已确认威胁”或其他。

状态:问题已识别且待解决

详细信息:1月15日引入了新的事件状态，磁贴没有考虑这些状态。新解决状态被解释为在进行中，因此，即使该突发事件使用其中一个新状态被关闭，它仍被视为进行中工作。

解决方法：无

后续步骤：无

预期分辨率：待定

思科集成

1. — 思科XDR — 思科安全终端集成链接在思科XDR门户上不起作用

状态:问题已识别且待解决

详细信息:在Admin > Integrations选项卡中，安全终端“启用”链接断开。点击enable按钮后，它会重定向到Threat Response页面，并循环到XDR组织选择器页面，而不是转到安全终端控制台。

解决方法：可以从思科安全终端门户执行集成

后续方案思科正在努力实施此问题的修复程序

预期分辨率：待定

2. Cisco XDR — 思科安全防火墙完全集成

详细信息：为了确保思科防御协调器(CDO)、安全服务交换(SSX)和安全分析和记录(SAL)之间的无缝集成，需要手动映射。此过程涉及联系思科TAC以执行必要的配置和映射。

解决方法：联系TAC，以协助关联相关客户并确保系统的正确集成。

预期分辨率：待定

第三方集成

1. — 具有G类型许可证的Microsoft客户无法使用XDR Microsoft集成。

状态：按设计工作

详细信息:Microsoft G类型授权仅在受控环境中为政府实体调配访问权限。

后续步骤：思科正在与Microsoft合作，以了解与提供Microsoft G类型授权的Microsoft GCC环境集成的要求。如果可行，思科XDR计划与Microsoft G类型许可证集成，用于Microsoft Defender for Endpoint、O365和EntraID。

预期分辨率：待定

资产

此XDR功能目前没有已知问题。

XDR自动化

1.- XDR自动事件自动化规则意外停止运行

状态：已确定问题和待解决问题

详细信息：由工作流程支持的事件自动化规则和触发器意外停止运行。在XDR用户界面中不会指明，除非查看随时间推移而运行的工作流的指标。执行此操作时，客户将看到工作流运行减少或为零，具体取决于问题持续的时间长短。

后续步骤：思科已将此问题确定为XDR后端中的一个问题，并正在设法解决该问题。思科还计划实施其他监控和状态跟踪功能，以避免将来发生此问题。

解决方法：禁用并重新启用规则以启动工作流规则触发和处理的重新启动。

预期分辨率：2025年3月

设备/传感器

1.- Cisco XDR-Analytics — 虚拟环境中的ONA安装失败，错误表示“校验和验证失败”
状态：已确定问题和待解决问题

详细信息:在虚拟环境中部署ONA传感器时，ISO无法完成安装过程并发生错误。

解决方法：使用Ubuntu ISO独立安装Ubuntu Server 24.04，并遵循advanced install步骤运行ONA as a service。使用7.0 U2兼容性

后续方案思科正在努力实施此问题的修复程序

分辨率：下一版XDR传感器版本

2.- Cisco XDR-Analytics - ONA传感器详细信息中的流量图表仅配置ETA探针时不会填充
状态：已确定问题和待解决问题

详细信息:Traffic Graph显示，当ONA仅配置了ETA探测时，没有流量。

解决方法：无

后续方案思科正在努力实施此问题的修复程序

3. — 思科XDR-Analytics — 来自思科遥测代理(CTB)的ETA遥测不用于填充ETA控制面板
状态：已确定问题和待解决问题

详细信息:由CTB生成或通过CTB上传并由其他设备生成的ETA遥测不会用于填充ETA控制面板

解决方法：将ONA与ETA探针配合使用

后续方案无

分辨率：下一版XDR传感器版本

安全客户端

要查阅有关安全客户端的问题，请遵循文章。

XDR-A

1. — 多个IP地址和/或多个主机名可以与XDR-A中的单个设备名称关联

状态:未解决/已推迟

详细信息:多个活动IP地址可以与SNA/XDR-A门户中的单个设备关联。这可以包括NVM和非NVM设备。某些设备也具有多个主机名。根据当前实施，设备注册可能导致设备具有多个IP地址（位置）。 其中一些IP地址可能来自用户的家庭网络，并且可能与组织网络中的IP地址冲突。

解决方案：目前没有解决此问题的方法，该问题在当前架构中仍然存在。人们希望，一旦实施新架构，将来这一问题可能会得到更好的解决，新架构将允许来自ONA和NVM的网络活动规范化为OCSF，并集中在一起。

后续方案不适用

解决方案：未来/待定

已解决的问题

1. — 标记任务不适用(Mark Task Not Applicable)选项仅在创建XDR事故时才会考虑，在更新事故时不会考虑。

状态：已解决

详细信息:Cisco XDR指导响应手册提供用于隐藏不适用于当前事件的任务的选项。2024年10月，思科对Cisco XDR发布了一项增强功能，用于自动隐藏没有适用可观察量的任务。此增强功能可在创建事故时使用，但在更新时不评估适用的任务。

后续步骤：已实施修复

如果需要联系思科支持，请按照此链接中提供的说明操作。

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）。