Cisco XDR Known Issues

Contents

Introduction

This article documents currently known technical issues for Cisco XDR.

Technical issues can be acknowledged by Cisco, under review, pending resolution, or deemed working as expected.

Known Issues:

Incidents

1.- Mark Task Not Applicable option is only considered on XDR Incident creation and not on Incident update.

> **Status:** Issue Identified and Pending Resolution
>
> **Details:** Cisco XDR Guided Response Playbooks provide the option to hide tasks that do not apply to the current incident. In October 2024, Cisco released an enhancement to Cisco XDR to automatically hide tasks with no applicable Observables. This enhancement works when an incident is created but does not assess applicable tasks when updated.
>
> **Next Steps:** Cisco is working to implement the fix for this issue
>
> **Expected Resolution:** December 2024

Investigations

No known issues for this XDR functionality at this time.

Cisco Integrations

No known issues for this XDR functionality at this time.

Third-Party-Integrations

1.- Microsoft customers with G-type licenses cannot utilize the XDR Microsoft integrations.

Status: Working as Designed

Details: Microsoft G-type entitlements are provisioned access in controlled environments for government entities only.

Next Steps: Cisco is working with Microsoft to understand the requirements to integrate with the Microsoft GCC environment in which Microsoft G-type entitlements are provided. If viable, Cisco XDR intends to integrate with Microsoft G-type licenses for Microsoft Defender for Endpoint, O365, and Entra.

Assets

No known issues for this XDR functionality at this time.

XDR Automate

1.- XDR Automate Incident Automation Rules unexpectedly stop running

Status: Issue Identified and Pending Resolution

Details: Incident Automation Rules powered by workflows and triggers unexpectedly stop running. This is not indicated in the XDR User Interface, except when reviewing the metrics for ***Workflows Run Over Time.*** When doing so, customers will see reduced or zero workflows run, depending on how long the issue has been ongoing.

Next Steps: Cisco has identified this as an issue within the XDR backend and is working to resolve it. Cisco also plans to implement additional monitoring and state-tracking features to avoid this issue from occurring in the future.

Workaround: Disable and Re-enable the rule to kick off a restart of the workflow rule triggering and processing.

Expected Resolution: January 2025

XDR Analytics

No known issues for this XDR functionality at this time.

Secure Client

1.- Secure Client / Endpoint deployments are impacted by a Microsoft Intune / Microsoft Defender for Endpoint updates, preventing proper installation

Status: Working as Designed

Details: Ongoing: This issue impacts Cisco XDR customers installing Cisco Secure Client for Network Visibility Module (NVM) usage with Cisco XDR. Microsoft Defender for Endpoint settings (configured via Intune) restrict Secure Client from properly installing. When a feature currently in preview in Microsoft Defender for Endpoint Attack Surface Reduction, ***Attack surface reduction - block use of copied or impersonated system tools (preview)***, is disabled, installation can occur.

Next Steps: Cisco Secure Client is behaving as expected when it attempts to install. However, Microsoft Defender for Endpoint / Microsoft Intune is causing unexpected interference with the installation. Cisco has identified a workaround for customers experiencing this issue.

Workaround: It is advised to consult the configuration for this feature with the application developer or consult this feature further through this knowledge base. For immediate remediation, we can either move our managed endpoint in Intune to a less restrictive policy or temporarily turn this feature explicitly off until proper steps are taken. This setting under the Intune admin portal was used as a temporary measure to restore Secure Endpoint connectivity.

For more details on this issue, please check this article.

If you need to contact Cisco Support, follow the instructions provided in this link.