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

No known issues for this XDR functionality at this time.

Investigations

No known issues for this XDR functionality at this time.

Control Center

No known issues for this XDR functionality at this time.

Cisco Integrations

1. Cisco XDR - Cisco Secure Firewall Full Integration

> **Details:** To ensure seamless integration between Cisco Defense Orchestrator (CDO), Security Services Exchange (SSX), and Security Analytics and Logging (SAL), manual mapping is required. This process involves contacting Cisco TAC to perform the necessary configurations and mappings.

Workaround: Contact TAC in order to assist in linking the relevant accounts and ensuring proper integration of the systems.

Expected Resolution: TBD

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 EntraID.

Expected Resolution: Resolved, integration available here.

Assets

No known issues for this XDR functionality at this time.

XDR Automate

No known issues for this XDR functionality at this time.

Appliances/Sensors

No known issues for this XDR functionality at this time.

Secure Client

In order to consult the issues for Secure Client, please follow the article.

XDR-Analytics

1. - Several IP addresses and/or multiple host names can get associated with a single device name in XDR-A

Status: Un-Resolved / Postponed

Details: Several active IP addresses can get associated with a single device within the SNA/XDR-A Portal. This can include both NVM and non-NVM devices. Some devices also have multiple hostnames. Based on the current implementation, the registration of devices could result in a device having more than one IP address (location). Some of these IP addresses might be from the user's home network and may collide with IP addresses in the organization's network.

Workaround: There is no work around for this issue at this time, and the issue still exists in the current architecture. There are hopes that this issue may be better addressed in the future, once new architecture is implemented which will allow for network activities from both sources ONA and NVM to be normalized to OCSF and brought together.

Next Steps: N/A

Resolution: Future / TBD

Tracking CDET: CSCwo67299

Resolved Issues

1.- Cisco XDR - Cisco Secure Endpoint integration link not working on Cisco XDR Portal

Status: Issue Identified and Pending Resolution

Details: In the Admin > Integrations Tabs the Secure Endpoint "Enable" Link is broken. Once we hit the enable button, it is redirecting to the Threat Response page and it loops to the XDR org selector page instead of going to the Secure Endpoint Console.

Workaround: Integration can be performed from the Cisco Secure Endpoint Portal

Next Steps: Cisco is working to implement the fix for this issue

Expected Resolution: This issue has been resolved.

2.- 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: Resolved.

3. - Cisco XDR-Analytics - ONA installation failure in Virtual Environments with an error indicating "***checksum verification failed***"

Status: Issue Identified and Pending Resolution

Details: When deploying a ONA sensor in a Virtual Environment, the ISO fails to complete the install process and errors out.

Workaround: Install Ubuntu Server 24.04 independently with the Ubuntu ISO and follow the advanced install steps to run ONA as a service. Use the 7.0 U2 compatibility

Next Steps: N/A

Resolution: This issue has been resolved in the latest build of the ONA Sensor

4.-MTTR tile on the Control Center shows inaccurate numbers for incidents that have been resolved using one of the new states such as "Closed: False Positive", "Closed: Confirmed Threat" or other.

Status: Issue Identified and Pending Resolution

Details: New incident states have been introduced on Jan 15th and the tile doesn't take those states into consideration. The new resolution states are interpreted as work-in-progress, so even if that incident has been closed using one of the new states, it is accounted for as work in progress.

Workaround: None

Next Steps: None

Expected Resolution: Resolved

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