M365 Defender Delete Export Settings

Last updated by | Naser Mohammed | Mar 19, 2023 at 7:18 AM CDT

Customer Cannot Delete Export Settings Rules

Context

Customer complains that the export rule cannot be deleted, or it seems like it was deleted but data still ingested

Impact

Data ingested into the log analytics MDE/MDO tables. User cannot stop data ingestion from the UX.

Possible Causes

This can be caused by either:

Workspace was deleted from Sentinel but the Export Settings was not deleted from Microsoft Defender 365 (Note: Currently the offboarding mechanism of Sentinel is not supporting Defender offboarding because sending rest request requires the customer token). User does not have permissions UX issue

Identifying the cause

Check if workspace exists Link to Query

WorkspacesMatadataView | where WorkspaceId = "<WorkspaceId>" or

Link to Query

WorkspacesMatadataView | where WorkspaceName = "<WorkspaceName>" Check whether Export Setting Rule exists in Microsoft Defender 365

Log in to Microsoft Defender for Endpoint portal as a Global Administrator or Security Administrator. Go to Data export settings page on Microsoft Defender Security Center. Look for a rule with name that starts with "SentinelExportSettings-" Check for errors in the user's debug console (browser) - Are there 403/Forbidden requests to windows defender? If so, the user doesn't have permissions to Microsoft 365 Defender. If user does not have global admin or security admin roles - use a user that has permissions

Check if the connector is connected in our UX Operations | where timestamp >ago(7d) | where Scenario == "DataConnectors" | where Context == "AzureSentinel/DataConnectorsBlade/DataProvider/FillingConnectorData/CheckingConnectivity/checkConnectorsConnectivity/GetAllConnectors/Trace" | where WorkspaceArmId contains "/subscriptions/f7fb6f38-a821-4b50-8f0f-9b100ec8cbd7/resourceGroups/rgprdsecops01la01/providers/Microsoft.OperationalInsights/workspaces/logcanadacentralprdsecops01" | extend MicrosoftThreatProtection = tostring(Dimensions.MicrosoftThreatProtection) | where notempty(MicrosoftThreatProtection) | extend MTPEnable = MicrosoftThreatProtection !contains "Not " | project timestamp,MTPEnable

Check if the user set or delete the settings from Sentinel's portal Link to Query : Operations | where timestamp > ago(7d) | where WorkspaceArmId contains "<workspace-name>" | where OperationName contains "DataExportSettings" and OperationName !contains "get" | project OperationName, timestamp

If the user already delete or update the "Data Export Settings", but it still configued (verified in step 3), it seems that the update/delete failed. Continue to investigate why.

Mitigation Steps

If Workspace was deleted, or UX is broken, you delete the export setting user ARM request. Follow the following steps: The customer can send a delete request to: https://api.security.microsoft.com/api/dataexportsettings/ <setting-name> <setting-name> is always SentinelExportSettings-<workspace-name> For example: https://api.security.microsoft.com/api/dataexportsettings/SentinelExportSettings-resourcegroupmiguel HTTP METHOD: Delete. User must be global admin or security admin for the tenant If user does not have global admin or security admin roles - Add permissions to user or use admin user. How to assign global admin role or security admin role