NG SIEM - Microsoft Defender for Cloud

Overview

The Microsoft Defender for Cloud(external, opens in a new tab or window) integration allows you to monitor security alert events and assessments. When integrated with Elastic Security, this valuable data can be leveraged within Elastic for analyzing the resources and services that users are protecting through Microsoft Defender.

Use the Microsoft Defender for Cloud integration to collect and parse data from Azure Event Hub, Azure REST API, and then visualize that data in Kibana.

Compatibility

The Microsoft Defender for Cloud integration uses the Azure REST API. It uses the `2021-06-01` API version for retrieving assessments and the `2019-01-01-preview` API version for retrieving sub-assessments.

How it works

For the **assessment** data stream, the `/assessments` endpoint retrieves all available assessments for the provided scope, which can be a Subscription ID or a Management Group Name. For each assessment, if sub-assessments are available, we will make another call to collect them. We will aggregate the results from both calls and publish them.

What data does this integration collect?

This integration collects log messages of the following types:

- `Event`: allows users to preserve a record of security events that occurred on the subscription, which includes real-time events that affect the security of the user's environment. For further information connected to security alerts and type, refer to the security alerts reference guide(external, opens in a new tab or window).
- `Assessment`: collect security assessments on all your scanned resources inside a scope from the Assessments(external, opens in a new tab or window) and Sub Assessments (external, opens in a new tab or window) endpoints.

Requirements

Collect logs from Azure Event Hub

- **Azure Event Hub** - Elastic recommends using one Azure Event Hub for each integration.

  Visit Create an Azure Event Hub to learn more. Use Azure Event Hub names up to 30 characters long to avoid compatibility issues.
- **Consumer Group** - We recommend using a dedicated consumer group for the Azure Event Hub input. Reusing consumer groups among non-related consumers can cause unexpected behavior and possibly lost events.
- **Connection String** - The connection string required to communicate with Azure Event Hubs. See Get an Azure Event Hubs connection string to learn more.
- **Storage Account** - The name of the storage account where the consumer group's state/offsets will be stored and updated.
- **Storage Account Key** - The storage account key will be used to authorise access to data in your storage account.

Collect Microsoft Defender Cloud logs via API

- **Client ID -** The client ID related to creating a new application on Azure.
- **Client Secre**t - The secret related to the client ID.
- **Tenant ID** - The tenant ID related to creating a new application on Azure.
- **Management Group Name** - The name of the management group. Provide either `Subscription ID` or `Management Group Name` as the scope for the request. If both are provided, then `Management Group Name` will take precedence.
- **Subscription ID -** The unique identifier for the subscription. Provide either `Subscription ID` or `Management Group Name` as the scope for the request. If both are provided, then `Management Group Name` will take precedence.

Conclusion

Integrating Microsoft Defender for Cloud with Elastic Security provides a powerful way to centralize and analyze your cloud security posture. By leveraging Azure Event Hub for real-time security event streaming and the Azure REST API for assessment data, you gain comprehensive visibility into the threats and vulnerabilities affecting your Azure resources — all within Kibana.

With the `Event` data stream capturing live security alerts and the `Assessment` data stream continuously evaluating your scanned resources at both the assessment and sub-assessment level, your team can detect, investigate, and respond to risks more efficiently.

To get the most out of this integration, ensure your Azure environment is properly configured with dedicated Event Hub instances, isolated consumer groups, and the appropriate API credentials (Client ID, Client Secret, and Tenant ID). Choosing the right scope — whether a Subscription ID or Management Group Name — will also determine the breadth of coverage across your organization's Azure resources.

Once set up, this integration serves as a foundational component of a broader cloud security monitoring strategy, enabling your security operations team to act on meaningful, contextualized data rather than navigating siloed tools.

Revision #1
Created 5 March 2026 07:21:37
Updated 6 March 2026 07:36:38