NG SIEM Microsoft Graph Activity Logs

Overview

Microsoft Graph Activity Logs capture API-level interactions with Microsoft Graph — including the identity of the caller, the resources accessed, permissions used, and the outcome. Forwarding these logs to Elastic gives security and operations teams a centralized platform for detection, alerting, and long-term retention.

Prerequisite

Azure Requirements

- An active Microsoft Azure subscription
- Microsoft Entra ID (Azure AD) tenant with at least one application registered
- Global Administrator or Security Administrator role to configure diagnostic settings
- Azure Event Hub namespace and Event Hub instance (Standard tier recommended)
- A dedicated Azure AD application for Elastic with appropriate API permissions

Required Azure AD Permissions

Parameter	Description
AuditLog.Read.All	Read all audit log data from Microsoft Graph
Directory.Read.All	Read directory data associated with activity records
User.Read.All	Resolve user display names and UPNs in enrichment
Policy.Read.All	Read conditional access and authorization policies

Azure App Registration

Register an Azure AD Application

- In the Azure Portal, navigate to Microsoft Entra ID > App registrations > New registration.
- Set the name (e.g., elastic-graph-logs-reader) and choose "Accounts in this organizational directory only".
- Click Register. Note the Application (client) ID and Directory (tenant) ID.

- Under Certificates & secrets, create a new client secret. Copy the secret value immediately.
- Under API permissions, add the permissions listed in Section 3.3 above, then grant admin consent.

Create an Azure Event Hub

- In the Azure Portal, navigate to Event Hubs > Create.
- Create a namespace (Standard tier) in your preferred region.
- Inside the namespace, create an Event Hub named insights-logs-microsoftgraphactivitylogs.
- Under Shared access policies, create a new policy with Listen permission for Elastic.
- Note the connection string — you will need this in Elastic Fleet.

Configure Diagnostic Settings in Entra ID

1. In the Azure Portal, go to Microsoft Entra ID > Diagnostic settings > Add diagnostic setting.
2. Name the setting (e.g., elastic-graph-activity-stream).
3. Under Logs, check MicrosoftGraphActivityLogs.
4. Under Destination, select Stream to an event hub and choose the namespace and Event Hub created above.
5. Click Save. Logs will begin flowing within 5–15 minutes.

> **Note: The MicrosoftGraphActivityLogs category may appear as a preview feature. Ensure the feature is enabled for your tenant under Entra ID > User settings > Manage what information is shown.**

Elastic Fleet Configuration

With the Azure application registered, the next step is to configure Elastic Fleet to deploy the Microsoft Graph Activity Logs integration.

> **To enable log collection from the Microsoft Entra ID, provide the following information to CyTech Support:**

- **Event Hub Name**
- **Consumer Group**
- **Connection String**
- **Storage Account**
- **Storage Account Key**

Conclusion

Integrating Microsoft Graph Activity Logs into Elastic gives your security and operations teams a powerful, centralized view of every API interaction occurring across your Microsoft 365 and Entra ID environment. What was previously a siloed audit stream within Azure becomes a first-class signal in your Elastic security ecosystem — queryable, correlatable, and actionable alongside all your other data sources.

By following this guide, you have established a reliable log pipeline from Microsoft Entra ID through Azure Event Hub into Elasticsearch, mapped raw Graph API telemetry to ECS fields for out-of-the-box detection compatibility, and laid the groundwork for long-term retention, compliance reporting, and threat hunting in Kibana.

As Microsoft continues to expand the Graph Activity Logs preview with richer metadata, this pipeline will grow in value without requiring significant re-architecture. The Event Hub ingest pattern is inherently scalable, and Elastic's data stream model ensures index management stays efficient as log volume increases.

Security visibility is only as strong as the signals feeding it. Microsoft Graph Activity Logs are one of the highest-fidelity sources of identity and access telemetry available in the modern enterprise — and with Elastic, you now have the tools to make the most of them.

Revision #1
Created 5 March 2026 07:25:09
Updated 12 March 2026 07:35:27