NG SIEM - Microsoft Defender XDR

Overview

This guide covers the full integration of Microsoft Defender XDR with the Elastic Stack. Microsoft Defender XDR is a unified extended detection and response platform that correlates signals across endpoints, identities, email, cloud apps, and cloud workloads. Bringing its data into Elastic enables centralized threat hunting, cross-platform correlation, and unified SIEM workflows alongside your other log sources.

Prerequisites

Microsoft Requirements

- An active Microsoft 365 Defender or Microsoft Defender XDR license
- Access to Microsoft Entra ID (Azure AD) to register an application
- Global Administrator or Security Administrator role to grant API permissions and admin consent
- (Optional) Microsoft Defender XDR Streaming API requires a Microsoft 365 E5 or equivalent license for real-time event streaming

Azure App Registration

The Elastic Agent authenticates to the Microsoft Graph Security API using OAuth 2.0 client credentials. If you do not already have an app registration, follow the steps below.

Step 1: Register the Application

- Go to portal.azure.com and navigate to Microsoft Entra ID > App registrations > New registration.
- Name the app (e.g., elastic-xdr-integration) and select Single tenant under Supported account types.
- Leave the Redirect URI blank and click Register.
- On the overview page, copy and save the Application (client) ID and Directory (tenant) ID.

Step 2: Create a Client Secret

- Go to Certificates & secrets > Client secrets > New client secret.
- Add a description and set an appropriate expiry period.
- Click Add and immediately copy the secret Value — it is only shown once.

> **Important Secret Visibility**: Azure only displays the secret value immediately after creation. If the page is refreshed or the value was not saved, you will need to generate a new secret. If you regenerate, remember to update the secret in all Elastic integrations that reference this app registration to avoid breaking existing data pipelines.

Step 3: Grant API Permissions

- Go to API permissions > Add a permission > Microsoft Graph.
- Select Application permissions and add the following:
- Click Add permissions.
- If also integrating Microsoft Defender for Endpoint data, additionally add WindowsDefenderATP > Application permissions: Alert.Read.All and Machine.Read.All.
- Click Grant admin consent for [Your Tenant] and confirm. Verify all permissions show Granted status.

Elastic Fleet Configuration

With the Azure application registered, the next step is to configure Elastic Fleet to deploy the MDE integration.

- Collect alerts and incidents using Microsoft Graph Security API
  - Client ID
  - Client Secret
  - Tenant ID

- Collect events using Azure Event Hub
  - Event Hub
  - Consumer Group
  - Connection String
  - Storage Account
  - Storage Account Key

- Collect vulnerabilities using Microsoft Defender for Endpoint API
  - Client ID
  - Client Secret
  - Tenant ID
  - Oauth2 Token URL

Conclusion

Integrating Microsoft Defender XDR with Elastic unlocks a truly unified security operations experience, bringing together telemetry from endpoints, identities, email, cloud apps, and cloud workloads into a single platform for detection, investigation, and response. By connecting the Microsoft Graph Security API to Elastic's SIEM and search capabilities, security teams gain correlated, cross-workload visibility that goes far beyond what any single Defender product can offer on its own. Whether you're leveraging prebuilt detection rules, building custom threat hunting queries, or streaming real-time events via the XDR Streaming API, this integration gives your SOC the context and speed needed to tackle modern multi-stage attacks — all from one place.

Revision #1
Created 5 March 2026 07:22:46
Updated 10 March 2026 04:35:28