SOC Management Defender for Endpoint (EDR) Integration

A step-by-step guide to Securus360's Microsoft Defender for Endpoint P2 (EDR) Integration

Overview

The Securus360 Cyber SOC has the ability to collect alerts from Microsoft Defender for Endpoint. These logs empower Securus360 to monitor and alert on potentially suspicious activity happening in your environment. For this to work, you will need to configure a few things within your Azure tenant. This document will walk you through that process.

Please note: Auditing must be enabled for your organization in order to ensure data collection. For more information, click here.

Configure a New Azure Application

1. Log in to https://portal.azure.com using your Office365 Global Administrator credentials. (E.g. an account that is marked as Global Administrator.)
2. Navigate to the **Azure Active Directory** option in the menu
3. Click **App Registrations** option in the left-hand menu
4. Next, click **New registration** in the top menu
5. Configure the options for this **App Registration** as shown below:
    a. **Name:** Securus360 Collection Service (Defender for Endpoint)
    b. **Supported account types:** Accounts in this organizational directory only (Your tenant only - Single tenant)
    c. **Redirect URI:** No value, not needed

 +1 (949) 266-6900 | support@securus360.com
100 Spectrum Center Drive, Suite 900, Irvine, CA 92618, USA | www.securus360.com

SOC Management Defender for Endpoint (EDR) Integration

Configure permissions for your app registrations

1. Select **View API permissions**
2. Click **Add a permission** and then **APIs my organization uses**
3. Type **WindowsDefenderATP** in the search and select **WindowsDefenderATP**
4. Select **Application permissions** and grant **Alert.Read.All access**
5. Click **Add permissions**
6. Now that permissions are configured, click on **Grant admin consent for [your tenant name]**

Create client secret keys & collect necessary IDs

1. Select **Certificates & secrets** from the left-hand menu
2. Once the page loads, click **New client secret**
3. On the pop out that appears, provide a **Description** of **Securus360 Collection Service (Defender for Endpoint)** and select the longest available expiration option (NOTE: Take note of this expiration date - a new key will need to be provided to Securus360 at that time)
4. Collect the **value** of the client secret that you created. To do this, copy and paste the value into a secure location – this will be your only chance to collect this information (NOTE: Securus360 will need the secret value, not the secret ID)
5. Navigate back to the **Overview**
6. Copy your **Application (client) ID** and **Directory (tenant) ID** to a secure location

Note: If you wish to secure this even further, such as encrypting the text file with 7-Zip, please provide Securus360 with the password to decrypt/extract the archive.

Once complete, please upload the file containing these values to the Sharepoint link provided by Securus360. Then send an email to **support@securus360.com** to let us know that it has been successfully uploaded. Securus360 will confirm we have received the file as quickly as possible. After we confirm receipt, you can then opt to securely delete the file from wherever it was saved locally, such as an internal disk or a flash drive.

 +1 (949) 266-6900 | support@securus360.com
100 Spectrum Center Drive, Suite 900, Irvine, CA 92618, USA | www.securus360.com

SOC Management Defender for Endpoint (EDR) Integration

Running Defender for Endpoint & Securus360 MXDR?

Please ensure the following exceptions are in place prior to installing agents

- C:\Windows\Sysmon64.exe (Note: No longer used starting with Agent version 2304.3.2 – can optionally be removed once all systems are on that version or higher)
- C:\Program Files\Elastic\Agent*
- C:\Program Files\Elastic\Agent\elastic-agent.yml
- C:\Program Files\Elastic\Agent\fleet.enc
- C:\Program Files\Elastic\Agent\data\elastic-agent-*\logs\elastic-agent-json.log
- C:\Program Files\Elastic\Agent\data\elastic-agent-*\logs\default*-json.log*
- C:\Program Files\Elastic\Endpoint\elastic-endpoint.exe
- C:\Program Files\Cerulean*

If you have any questions or concerns regarding this procedure, please reach out to either your preferred contact or to **support@securus360.com**

Lastly, if you would prefer a different method of sending us this information, Securus360 is more than willing to accommodate whichever method adheres to your preferences and security policies.

 +1 (949) 266-6900 | support@securus360.com
100 Spectrum Center Drive, Suite 900, Irvine, CA 92618, USA | www.securus360.com