Microsoft Defender End Point

|  |  |  |
| --- | --- | --- |
| **S. No** | **Table Name** | **API** |
| 2 | Alerts | <https://api.securitycenter.windows.com/api/Alerts?$filter=alertCreationTime gt 2019-08-01T18:30:00Z> |
| 3 | Machine All State | https://api.securitycenter.microsoft.com/api/machines?$filter=lastSeen gt 2022-01-01Z |
| 6 | Device AVinfo | <https://api.securitycenter.microsoft.com/api/deviceavinfo> |

**Overview:**

Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.

Defender for Endpoint uses the following combination of technology built into Windows 10 and Microsoft's robust cloud service:

* **Endpoint behavioral sensors**: Embedded in Windows 10, these sensors collect and process behavioral signals from the operating system and send this sensor data to your private, isolated, cloud instance of Microsoft Defender for Endpoint.
* **Cloud security analytics**: Leveraging big-data, device learning, and unique Microsoft optics across the Windows ecosystem, enterprise cloud products (such as Office 365), and online assets, behavioral signals are translated into insights, detections, and recommended responses to advanced threats.
* **Threat intelligence**: Generated by Microsoft hunters, security teams, and augmented by threat intelligence provided by partners, threat intelligence enables Defender for Endpoint to identify attacker tools, techniques, and procedures, and generate alerts when they are observed in collected sensor data.

In general, you'll need to take the following steps to use the APIs:

* Create an [AAD application](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/exposed-apis-create-app-nativeapp)
* Get an access token using this application.
* Use the token to access Defender for Endpoint API

You can access Defender for Endpoint API with **Application Context** or **User Context**.

* **Application Context: (Recommended)**

Used by apps that run without a signed-in user present. for example, apps that run as background services or daemons.

Steps that need to be taken to access Defender for Endpoint API with application context:

* 1. Create an AAD Web-Application.
  2. Assign the desired permission to the application, for example, 'Read Alerts', 'Isolate Machines'.
  3. Create a key for this Application.
  4. Get token using the application with its key.
  5. Use the token to access the Microsoft Defender for Endpoint API
* **User Context:**

Used to perform actions in the API on behalf of a user. Steps to take to access Defender for Endpoint API with user context:

* 1. Create AAD Native-Application.
  2. Assign the desired permission to the application, ex: 'Read Alerts', 'Isolate Machines' etc.
  3. Get token using the application with user credentials.
  4. Use the token to access the Microsoft Defender for Endpoint API

**Report Design Requirements from AbuAyshe Nabil:**

1. How many devices in the firm
2. How many devices has an agent
3. how many in the network and agent not working (Active - No Sensor)
4. last signature update
5. how many machines got infected (Malware not Cleared)
6. How many machines in the network and doesn't have AV

**Data Last Refreshed date:**

Added a date column at the top right corner in the Machines page.

**Device Info:**

1. Use web or OData Feed or blank Query. To import the data using the API <https://api.securitycenter.microsoft.com/api/deviceavinfo>.
2. Expand Necessary columns and remove unwanted or null columns.

**Machine All State**

1. Use web or OData Feed or blank Query. To import the data using the API (Date filter is not fixed) [https://api.securitycenter.microsoft.com/api/machines?$filter=lastSeen gt 2022-01-01Z](https://api.securitycenter.microsoft.com/api/machines?$filter=lastSeen%20gt%202022-01-01Z)
2. Expand Necessary columns and remove unwanted or null columns.

**Alerts:**

1. Use web or OData Feed or blank Query. To import the data using the API (Date filter is not fixed) [https://api.securitycenter.windows.com/api/Alerts?$filter=alertCreationTime gt 2019-08-01T18:30:00Z](https://api.securitycenter.windows.com/api/Alerts?$filter=alertCreationTime gt 2019-08-01T18:30:00Z%20)
2. Expand Necessary columns and remove unwanted or null columns.

Create a Connection among all tables using “Id” or “machine Id” and should be one direction. IF you need any permissions Ask Amit Rai and Nabil A.

Below are the two pages in the dashboard.

**Score card details:**

1. **High Exposure:** Count of id where the condition is exposure level = High
2. **Devices:** Count of id where the osPlatform=windows and onboardingstatus= onboarded and can be onboarded
3. **Devices without AV:** Count of id where the **osPlatform**=windows and **onboardingstatus**= canbeonboarded
4. **Devices with AV:** Count of id where the **osPlatform**=windows and **onboardingstatus**= onboarded
5. **Last Signature Updated:** Latest date of avSignatureUpdateTime.
6. **High Risk:** Count of Id where the filter is Risk Score is equal to high.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated