MICROSOFT SENTINEL

Import of Threat Intelligence Indicators From a Flat File

NDA Private Preview | Participant Resources & Preview Scope v1.0

Start: May 11, 2022 Est. Duration: 4 weeks Complexity: Less than 1 hour of effort

Description

This feature will enable Microsoft Sentinel customers to import threat intelligence indicators from a flat file like CSV and JSON files. This is an easy way to ingest indicators of compromise, that you may have from peer analysts or files of indicators on the web, into Sentinel.

Common Use-Cases & Scenarios:

- Customers who are looking to import threat intelligence indicators from a flat file like CSV and JSON files.

Preview Prerequisites

Aspect	**Details**
Required/Preferred Environmental Requirements	• The customer workspace needs to be in 1 of these regions: ○ West Europe ○ East US ○ Central US
Required Roles & Permissions	N/A
Clouds	✓ Commercial Clouds ✗ Nation/Sovereign (US Gov, China Gov, Other Gov)

Feature-flag URL

Use this URL to enable the feature in your environment: https://portal.azure.com/?feature.fileimports=true#blade

Preview Instructions

Using this feature you can import indicators of compromise from a flat file. To do so, please follow these steps, or watch our pre-recorded demo here.

1. Go to the Azure portal using the feature flag URL provided in this document.
2. Click on “Microsoft Sentinel” and visit the “Threat Intelligence” menu under “Threat Management”.
3. Click on “Import” and then click on “Import external file”.
4. On the Import from a file panel on the right, select the format of the file.
5. You can download the template for the indicators. Sentinel has one template for all other indicators like ip address, url, domains etc. and one template for file type indicators.
6. Fill in the required values for indicators in the CSV/JSON template and upload the file.

7. Provide a source for the indicators. This is the value that gets stamped on each indicator in the "SourceSystem" field.
8. Microsoft Sentinel provides you an option to import partial indicators if your file conveys invalid indicators. Select the option of "Import the valid indicators" from the "If there are invalid indicators" field if you would like to do so.
9. Click "Import".
10. To manage your file imports and see the status of your import, click on "Import" and "Manage file imports". You can download your error files detailing the errors with invalid indicators on this screen.

Notes:

1. Microsoft Sentinel supports indicators with **observable_types** as ipv4-addr, ipv6-addr, domain-name, url, user-account, email-addr, windows-registry-key.
2. *Severity* can accept values between 0 and 5.
3. *Confidence* can accept values between 1 and 100.
4. *tlpLevel* can accept values of "white", "green", "amber", "red".
5. "*valid_from*" date needs to be before the *"valid_until*" date.

Share Your Feedback

Please respond to this feedback survey after testing this feature. Also, in this survey you can volunteer to join Rijuta Kapoor, this feature's PM owner, on a 1:1 dive to learn gather your feedback in more detail. We only have five spots available; candidates must commit to using this feature for one week.

Known Issues / Limitations

- This private preview will only be offered in the West Europe (WEU), East US (EUS), Central US (CUS) regions to start. Other regions will be added once this feature is announced as private preview.
- During this preview, RBAC is not supported. However, it will be supported once this feature moves to public preview.

Key Contacts

Feature PM: Rijuta Kapoor | Rijuta.Kapoor@microsoft.com
Private Preview PM: Pablo Chacón (HE/HIM) | Pablo.Chacon@microsoft.com

Thank you! Your participation is a vital part of our Cloud + AI Security product development process.

Microsoft