

CONFIGURE ASSESSMENTS

This feature is released as a Public Preview. Pre-GA products and features are available "as is" and might have limited support. For more information, please contact your TSC, your CSM, or go to [Support](https://docs.mandiant.com/home/mandiant-support-cases). (<https://docs.mandiant.com/home/mandiant-support-cases>)

You can configure an Assessment, which contains a set of security content that you specify (any combination of Actions, Sequences, and Evaluations). This Assessment can then be distributed to other Director instances, from which the bundled content can be run.

From a Director, you can create Assessments in either of the following ways:

- Create a brand new Assessment directly using configuration options on the Director.
- Import an existing Assessment provided by an administrator of another Director.

Configure a New Assessment

1. Go to **Library > Assessments**.
2. Select **Create Assessment**.
3. Provide a **Name** and **Description** to identify the Assessment.
4. Specify an **External Reference** if you want to use a custom naming system to easily identify this Assessment. You can enter any text in the field. If you give multiple Assessments the same external reference, you can group them under this metadata. This reference value also appears in the data that is published through a Pipeline to an external data visualization tool, such as Power Bi.
5. (Optional) If required, check **Assign a Due Date** and specify a due date in the drop-down.



The due date must set to the day on which you're creating the Assessment or a future date. You cannot select a past due date.

6. Select **Add Content** and choose a content type (Actions, Sequences, or Evaluations) you want to add to the Assessment.
7. (Optional) As you click through content, select **View Details** to load the content information inline. When finished reviewing, select **Back to List**.

Add Actions To Assessment
✕

[← Back To List](#)

Action Details

VID: A102-106 V6.0.0
 Created: 2020-08-19 01:30:14 UTC
 Modified: 2022-08-31 17:07:06 UTC

Name
 Application Vulnerability - APT41, Citrix CVE-2019-19781, Reconnaissance

Description
 This Action demonstrates the initial POST request used to exploit the Citrix Application Delivery Controller (ADC) and Citrix Gateway. This vulnerability, assigned CVE-2019-19781, allows an unauthenticated attacker to perform arbitrary remote code execution via directory traversal.

The commands executed on the vulnerable host can be seen inside the request body. In this Action, the command executed is file /etc/pwd.

According to Mandiant Threat Intelligence, APT41 has exploited the vulnerability in order to gain an initial foothold in a targeted environment. APT41 executed the same command against its targets with the possible objectives of determining whether or not the target was vulnerable and also to potentially return architecture-related information that would help to successfully deploy backdoors to the host. More information on APT41's techniques can be read about in report: 20-00005182.

Note: For testing purposes, this Action is demonstrated over HTTP. Real-world attacks are most likely to occur over HTTPS.

Tags
APT41
CVE-2019-19781
CWE:200
CWE:522


MITRE ATT&CK

Technique	ID	Tactics	Actions
Remote System Discovery	T1018	Discovery	🔄

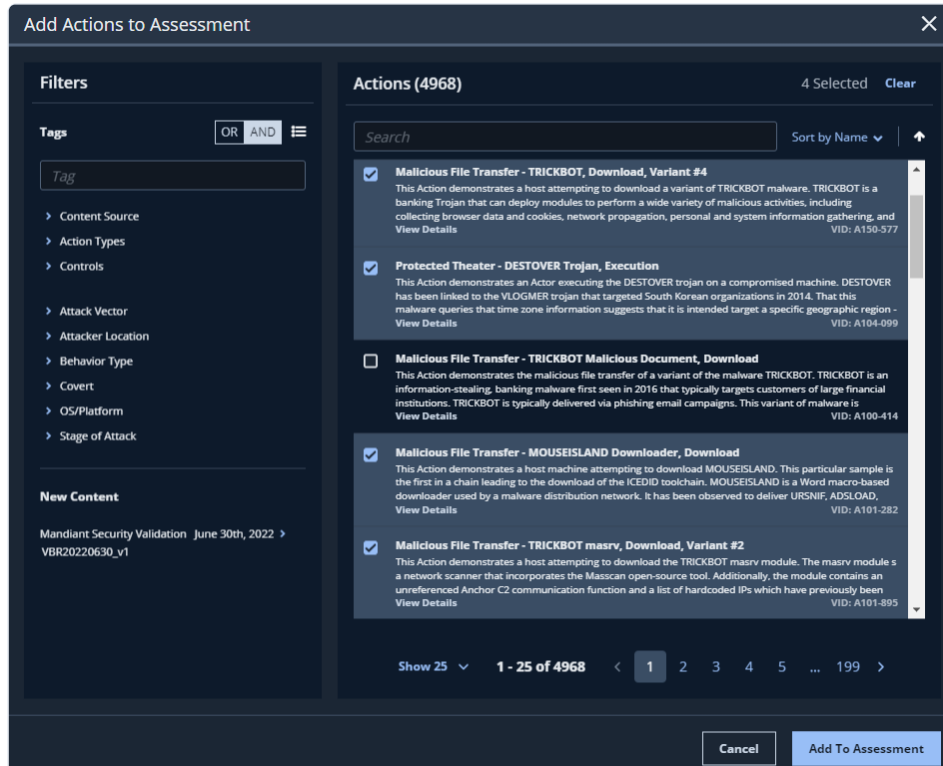
Run As Tags
 None

Viewing Content Details Inline

8. When you've chosen all the content, select **Add to Assessment**.




In any of the three content type windows, you can select multiple entries at once to add these to the Assessment. You can also select **Clear** if you selected an incorrect entry and want to start over.



Adding Actions in Bulk to an Assessment

9. Repeat the Add Content steps (6 - 9) for any other types of content that you want to add. The categorized content entries appear in the **Content to Run** section.



Added Content Example: Four Actions and Two Sequences

10. When you've added all the content, select **Save**. The Assessment appears in the list with a **Created** status.

Import an Existing Assessment

1. Go to **Library > Assessments**.

2. Select **Import Assessment**.
3. Browse to and select the local Assessment file (in JSON format) that was exported from another Director.
4. Select **Import**. The Assessment appears in the list with an **Imported** status.



- You cannot edit an imported Assessment. If you need to, you can clone the Assessment to create a new one.
- For an imported Assessment, if any of its security content (Sequences, Evaluations, Actions) is not present on the receiving Director, there might be an error message or no message at all, depending on the version of Security Validation.