Mandiant

SECURITY VALIDATION ACTIONS

Overview

You view and create Actions by going to **Library** > **Actions**. By default, the Validation Platform contains a large selection of Actions that are categorized by Filters and Dimensions. Refer to **Security Content Filters and Dimensions (https://docs.mandiant.com/home/security-content-dimensions)** for the full list of options.

The Action Library includes a text-based search that lets you sort Actions by Name, VID, Modified, Last Added, Last Run, and Total Runs in the Actions pane. You can choose the sort option from the Sort drop-down list next to the Search box. The sorting option you choose determines the order of the Actions:

- **Name**: Displayed in alphabetical order
- **VID**: Displayed numerically by VID
- **Modified**: Displayed by the date they were last modified
- **Last Added**: Displayed by the date when they were last added to the Director (for two weeks, they appear with a New status)
- **Last Run**: Displayed based on when they last ran
- **Total Runs**: Displayed based on how many times they ran

This video walks you through an example of running a port scan Action.

You can click the Sort drop-down list arrow to change the order of the Actions results from ascending to descending or descending to ascending.

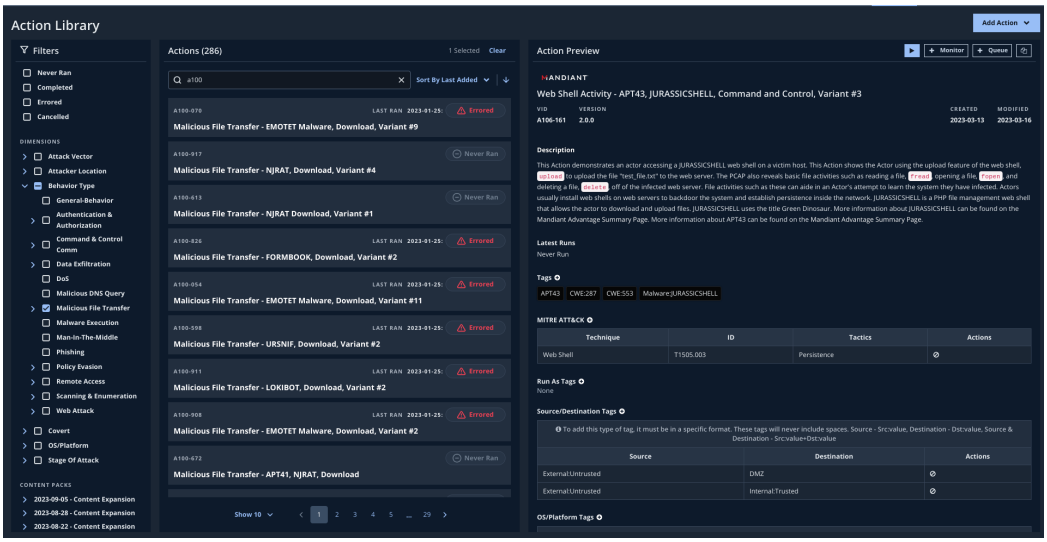
Once you set the sorting preferences for Actions in the Action Library, the sorting preferences set in **User** > **User Preferences** > **Content Settings** are only used in the Evaluations and Sequences libraries and API. The sort selection that you apply to the Action library is remembered and applied the next time you open the Library.

You can filter the list of Actions by Dimensions, Tags, and content packs.

- When filtering using the Tags, you select one or more tags and use AND & OR to focus the search.
- When filtering using content packs, you choose new or updated Actions from any of the content packs that were released in the past 90 days.
  - Content is considered **New** if the selected content release was when Action was added to the library.
  - Content is considered **Updated** if the selected content release includes a modified version of an Action that was already in the library (it was added by a previous content import)
  - An Action that was Retired (removed from the library by a content import) no longer appears in the library

If you specify a MITRE ATT&CK Technique or Sub-Technique in the URL, the Action Library will automatically filter based on the relevant ATT&CK Tags. Use `/manage_sims/actions?attack_techniques=T####` to filter for Technique Tags or `/manage_sims/actions?attack_techniques=T####.###` to filter for Sub-Technique Tags.

You can create a .csv that captures all Actions in your Library. See **Creating a .csv of all Actions (https://docs.mandiant.com/home/creating-a-csv-of-all-actions)** for information.



Security Content - Actions

Understanding the Action Preview Pane

If you are reviewing Actions and trying to learn more about them, you need to understand an Action's Preview pane, which is displayed when you select an Action in the library, click an Action in Job Results, or click on an Action that's part of the Action Queue, an Evaluation, or a Sequence. The Action Preview pane lets you view important information about an Action before you run it and displays the Action's:

- Name & version
- Creation and modified dates
- Description
- Security Validation and User Tags
- Relevant MITRE Mitigations and NIST 800-53 Controls
- Dimensions
- Action-specific details (file dependencies, commands, ports used, etc)
- Related Event Filters
- Sequences and Evaluations that use the Action
- Common Detection Alerts.

When you select an Action, you see that Action's VID added to the Action Library's URL. You can use the `/manage/sims/action/<VID>` format to quickly view Actions by replacing the VID in the URL or bookmarking the URL.

The following sections provide additional information.

Version, Creation, and Modified Dates

There are a few differences you should understand when reviewing Mandiant-provided Actions versus user-created or imported Actions:

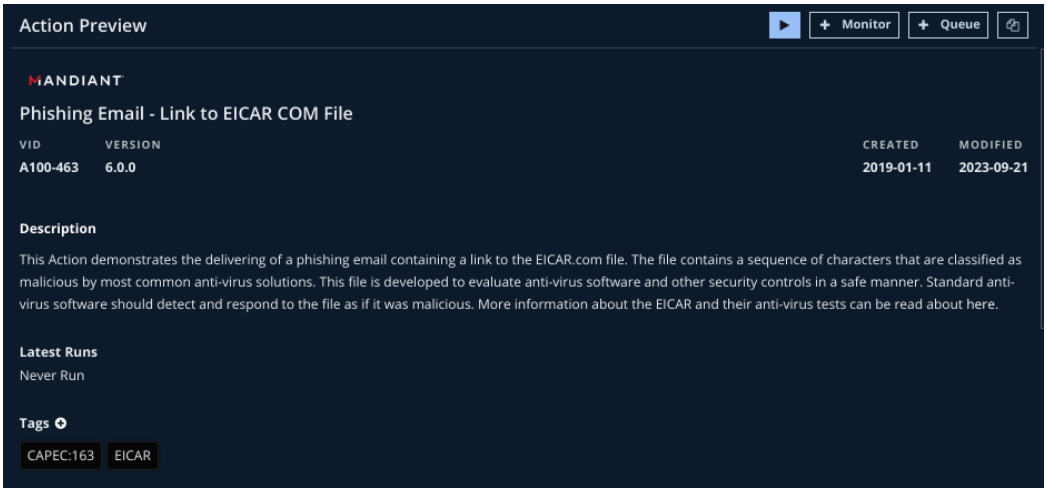
- **User-created or imported Actions**: The version and modified date updates when you modify the Action's tags, dimensions, and Action details.
- **Validation Platform Actions**: The version and modified date only update when the Security Validation team provides a new version of the Action.

Action Tags

The Action Tags sections provide information about what the Action is related to. Sections include:

- Tags
- MITRE ATT&CK Tags
- Run As Tags
- Source/Destination Tags
- OS/Platform Tags
- Control Tags

See **Action Tags (https://docs.mandiant.com/home/msv-action-tags)** for more information.

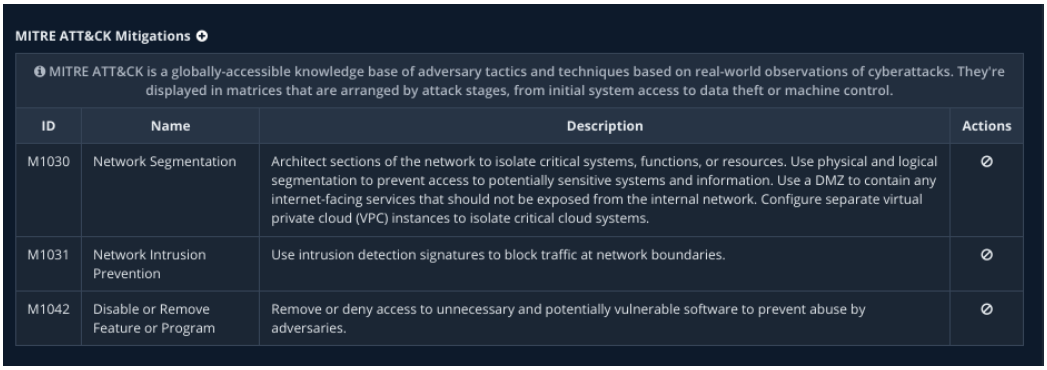


Tags in the Action Preview

MITRE ATT&CK Mitigations

The MITRE ATT&CK Mitigations section provides a table of MITRE ATT&CK Mitigations associated with the Action. This includes:

- MITRE Mitigation ID
- Name
- Description
- Whether you can remove the Mitigation or not (Actions)



The MITRE ATT&CK Mitigations section of the Action Preview

Click ⊕ to open a drop-down list and add other Mitigations to the table. You can only add Mitigations from that list. To remove a Mitigation you've added, click ✖ in the Actions column. You can only remove Mitigations that you have added to the Action.

NIST 800-53 (Rev. 4) Controls

The NIST 800-53 (Rev. 4) Controls section provides a table of NIST 800-53 Controls associated with the Action. Currently, the Validation Platform includes the AC, AU, AT, CM, CP, and IA Control Families. The table includes:

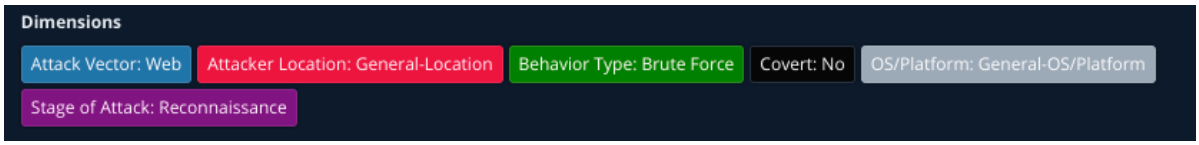
- Control number
- Control family
- Control
- Priority
- Whether you can remove the Control or not (Actions)

The NIST 800-53 (Rev. 4) Controls section of the Action Preview

Click ⊕ to open a drop-down list and add other Controls to the table. You can only add Controls from that list. To remove a Control you've added, click ✖ in the Actions column. You can only remove Controls that you have added to the Action.

Dimensions

The Dimensions section provides information that helps you categorize the type of Action. See for information about the dimensions.



Dimensions section in an Action's Preview

Action Dimensions

Dimension	Description
Attack Vector	The method the Validation Platform will use to process the Action
Attacker Location	Where the Action will attack from
Behavior Type	What kind of behavior the Action will process
Covert	Is the network traffic encrypted

Dimension	Description
OS/Platform	The operating system or platform the Action is designed to run on
Stage of Attack	The attack life cycle stage that the Action's belongs to

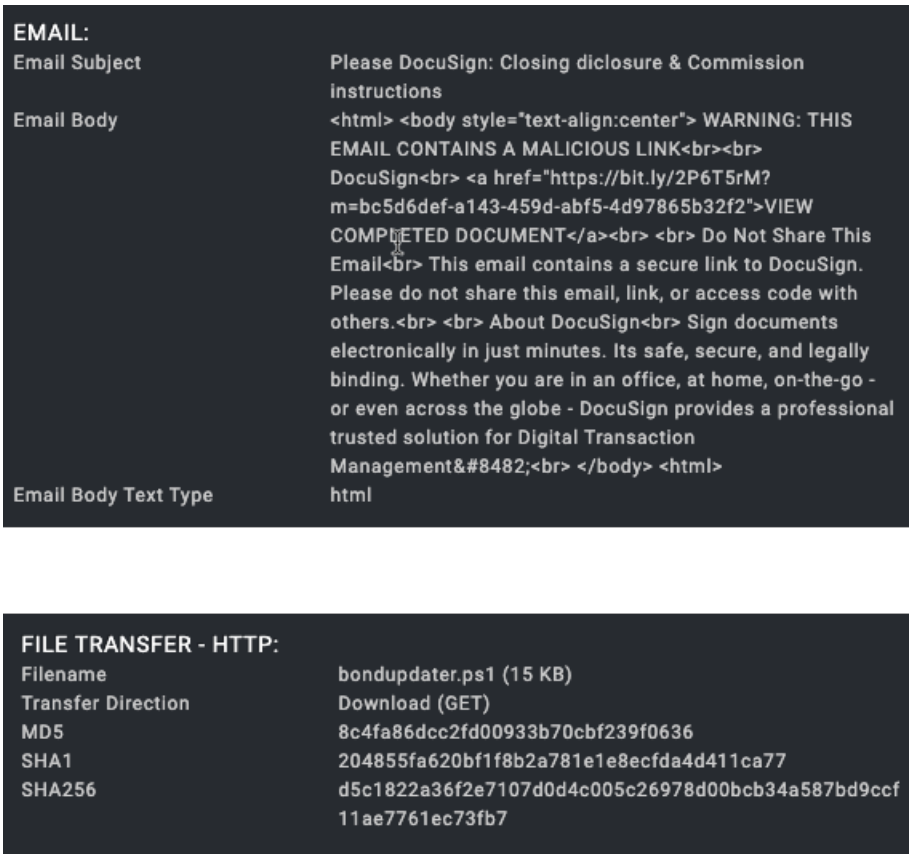
The platform also groups Actions together based on Content Source, Action Type, and Controls tested. This information isn't included in the Action preview, but is used in the Action Library's Dimension Filters.

Refer to **Security Content Dimensions** **(https://docs.mandiant.com/home/security-content-dimensions)** for the full list of the Security Validation Action Dimensions.

Action Details

Depending on the Action Type, information about files and tactics used in the Action displays under Dimensions and Tags. This can include:

- PCAP used in the Action that you can view in the platform or download. The PCAP section also displays whether a hexdump or HTTP traffic are included in the file.
- Port scan information, including which ports the Action will scan, the amount of time waited between scanning ports (Seconds to Sleep), and whether or not ports are checked in a randomized order.
- DNS query information, including query type, domain, and domain server used.
- Email overview information, including the email subject and body contents, email body text type, and name of email file attachments.
- Host CLI commands and supplementary information. This includes the specific commands included in the Action, file dependencies, seconds to wait after delivering files, what happens if files are removed during the wait period, and what happens if a destination file exists.
- File transfer information, including the file name and size, transfer direction, MD5 hash, SHA1 hash, and SHA256 hash.



EMAIL:	
Email Subject	Please DocuSign: Closing diclosure & Commission instructions
Email Body	<html> <body style="text-align:center"> WARNING: THIS EMAIL CONTAINS A MALICIOUS LINK DocuSign VIEW COMPLETED DOCUMENT Do Not Share This Email This email contains a secure link to DocuSign. Please do not share this email, link, or access code with others. About DocuSign Sign documents electronically in just minutes. Its safe, secure, and legally binding. Whether you are in an office, at home, on-the-go - or even across the globe - DocuSign provides a professional trusted solution for Digital Transaction Management™ </body> <html>
Email Body Text Type	html

FILE TRANSFER - HTTP:	
Filename	bondupdater.ps1 (15 KB)
Transfer Direction	Download (GET)
MD5	8c4fa86dcc2fd00933b70cbf239f0636
SHA1	204855fa620bf1f8b2a781e1e8ecfda4d411ca77
SHA256	d5c1822a36f2e7107d0d4c005c26978d00bcb34a587bd9ccf11ae7761ec73fb7

An Email and File Transfer Action Details section, taken from two different Action Previews

Cloud Action Details

The following fields display in the Action Preview pane for Cloud Actions (these fields / tables are specific to Cloud Actions):

- Name / Value pair inputs: Lists the name of the input(s) and default value(s)
- Name / output parameters: Lists the name of the output parameters, if available
- File Dependencies: Files that can be uploaded during creation or editing of Cloud Actions

> File names must be unique per File. For example, if you attach two files with the name `my_file` to the same Action, the Action fails to create and you receive an error saying that the names must be unique. However, you can use the same file name on two separate Actions.
>
> The file should be available as a variable in the python script. If you attach a text file, you should be able to read the contents by using `FILE_DEPENDENCIES['variable_name'].decode('utf-8')` in the script.

- Python script text for the Cloud Action: Scripts that comprise the Setup, Malicious Action(s), and Cleanup scripts for the Cloud Action

Setup

```python
import boto3
import botocore
import logging
import time


def s3_create_bucket(bucket_name):
    s3_client = boto3.client('s3')
    res = s3_client.create_bucket(
        ACL='public-read',
        Bucket=bucket_name
    )
    if res["ResponseMetadata"]["HTTPStatusCode"] == 200:
        logging.info("Created bucket")
        return res["ResponseMetadata"]["RequestId"],res
    else:
       raise Exception("HTTP Error: {}".format(res["ResponseMetadata"]["HTTPStatusCode"


def s3_put_object(file_bytes,bucket_name,s3_key):
    s3_client = boto3.client('s3')
    res = s3_client.put_object(
        Body=file_bytes,
        Bucket=bucket_name,
        Key=s3_key
    )
    if res["ResponseMetadata"]["HTTPStatusCode"] == 200:
```

Example of Setup Python Script for Cloud Action

Exfiltration from S3 Bucket

```python
import boto3
import botocore
import logging
import hashlib


Blocked_Errors = [
        "UnauthorizedOperation",
        "AccessDenied",
        "AuthFailure",
        "InvalidClientTokenId"
    ]


def s3_get_object(bucket_name,s3_key):
    s3_client = boto3.client('s3')
    res = s3_client.get_object(
            Bucket=bucket_name,
            Key=s3_key
    )
    res_code = res["ResponseMetadata"]["HTTPStatusCode"]
    if res_code == 200 or res_code == 204:
        logging.info("Object retrieved from bucket")
        return res["ResponseMetadata"]["RequestId"],res["Body"]
    else:
       raise Exception("HTTP Error: {}".format(res["ResponseMetadata"]["HTTPStatusCode"
```

Example of Malicious Python Script for Cloud Action

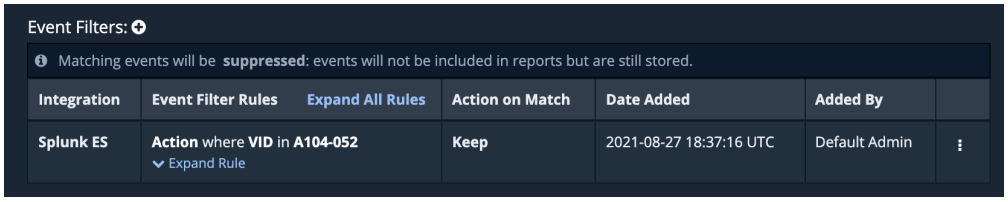
Cleanup

```
def s3_delete_object(bucket_name,s3_key):
    s3_client = boto3.client('s3')
    res = s3_client.delete_object(
        Bucket=bucket_name,
        Key=s3_key
    )
    res_code = res["ResponseMetadata"]["HTTPStatusCode"]
    if res_code == 200 or res_code == 204:
        logging.info("Object deleted")
        return res["ResponseMetadata"]["RequestId"],res
    else:
       raise Exception("HTTP Error: {}".format(res["ResponseMetadata"]["HTTPStatusCode"


try:
    if MSV_CLEANUP_OBJECT:
        s3_delete_object(NEW_BUCKET_NAME,S3_FILE_KEY)
    if MSV_CLEANUP_BUCKET:
        s3_delete_bucket(NEW_BUCKET_NAME)
    logging.info("Cleanup successful")
except:
    logging.error("WARNING: Error in cleanup, please delete bucket manually")

if not (MSV_CLEANUP_OBJECT or MSV_CLEANUP_BUCKET):
    logging.info("Cleanup not required")
```

Example of Cleanup Python Script for Cloud Action

Event Filters

The Event Filters section displays any Event Filter Rules that include the Action. Depending on your permissions, you can also Edit existing filters and create new ones.



The Event Filters section of the Action Preview

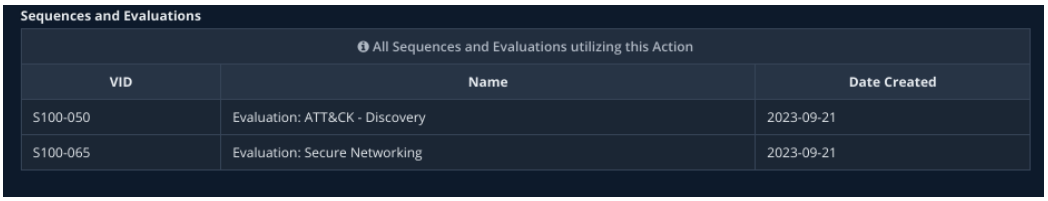
For full details, see **Event Filter Rules** (https://docs.mandiant.com/home/event-filter-rules).

Sequences & Evaluations

The Sequences and Evaluations section provides a table of each Sequence and Evaluation that uses the Action. The table includes:

- VID
- Name
- Creation date

See **Sequences & Evaluations** (https://docs.mandiant.com/home/msv-sequences-evaluations) for information.

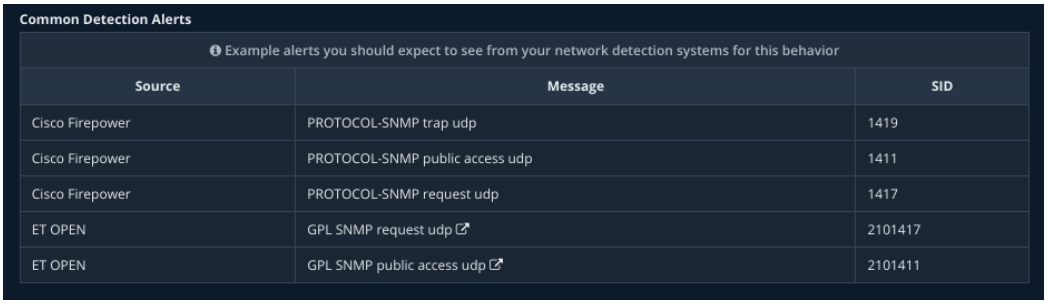


The Sequences and Evaluations section of the Action Preview

Common Detection Alerts (CDAs)

The Common Detection Alerts (CDAs) section is list of alerts that may fire in your security controls. CDAs are only applicable to network-based Actions. The CDAs are listed in a table that includes:

- The alert source
- The message expected to fire
- The Signature ID (SID), which is assigned by the vendor



The Common Detection Alerts section of the Action Preview