Mandiant

ACTION TAGS

Actions include several types of tags. These tags provide additional information about what the Action is related to (malware, TTPs such as MITRE ATT&CK Mitigations, Tactics, Techniques, and Threat Actors), offer guidance on how to run the Action and provides information about the type of controls that are tested. You can add your own tags to each of these tag types.

User Tags further refine the content. For example, a Sequence that models behaviors associated with TeslaCrypt ransomware, can be tagged with "TeslaCrypt" and "Ransomware". All Actions that are included in that Sequence can include the same tags. Tags are searchable and may be used in various reports.

This video walks you through a scenario for confirming you're protected against a ransomware attack. The walkthrough demonstrates the value of tags for isolating Actions with a common set of characteristics.

Users can create tags that are the same as Validation Tags. When you filter content using tags, the tag will only appear once. However, the filter results include content that has either a Validation Tag or User Tag that matches the filter.

Tags

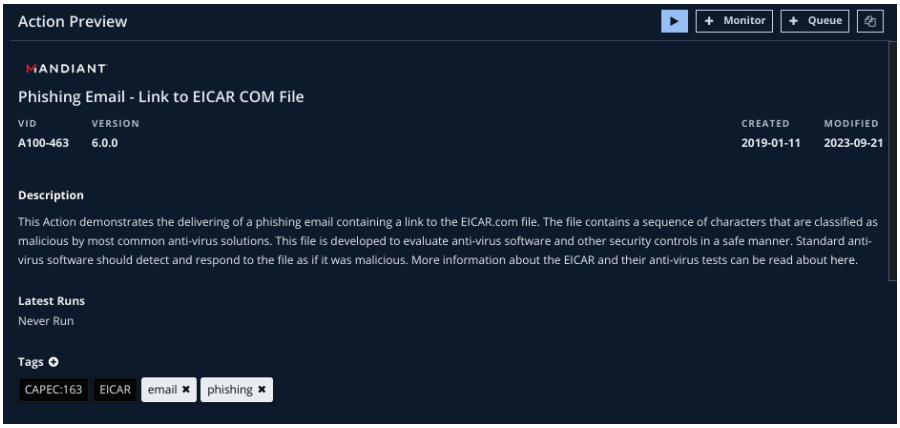
In this section, you find tags that categorize the Action. These tags could include MITRE ATT&CK Mitigations, Tactics, Techniques, and Sub-Techniques as well as other TTPs, NIST 800-53 controls, malware families, CVEs, and Threat Actors. When you add tags, you should use the following formats.

Tag category	Recommended Format
MITRE ATT&CK Mitigations	ATT&CK:*MITIGATION* (no spaces)
MITRE ATT&CK Tactics	ATT&CK:TA####
MITRE ATT&CK Techniques	ATT&CK:T####
MITRE ATT&CK Sub-Techniques	ATT&CK:T####.###
NIST 800-53 Controls	NIST:*CONTROL* (no spaces)
Malware families	Malware:*MALWARE_FAMILY* (no spaces)
CVEs	CVE-*YYYY-###*
Threat Actors	*THREAT_ACTOR*
General	*GENERAL*

When in doubt, use Tags to search for a Validation Tag and follow that format. You can add User Tags that are the same as Validation Tags.

To add this type of tag, enter a new tag. If the tag is already created, you can select it; otherwise, you click **Create Tag**. The

tags you enter or add appear with a white background. They can also be found on the Tags Settings page in the User Tags section.



User Tags on an Action

MITRE ATT&CK Tags

MITRE ATT&CK Tags show which MITRE ATT&CK Tactics, Techniques, and Sub-Techniques are associated with the Action. ATT&CK v12 Tags appear in a table that shows the Tactic, Technique / Sub-Technique, and Tactic ID. The Security Validation VRT use these tags when creating content, but you can also search for and add MITRE ATT&CK Tags to an Action.

There is an **Advanced Setting** (https://docs.mandiant.com/home/msv-advanced-settings) that allows you to define which version of the MITRE ATT&CK tags are used. By default, this is set to display the current version but you can manually update it to any version between 6.0 and the current version. You can also still view Actions based on different versions of the ATT&CK Tags using the Security Validation **API** (https://docs.mandiant.com/home/msv-api-4840).

MITRE ATT&CK Tags on an Action

Run As Tags

Run As Tags suggest the account type or role that should be used to run the Action. The tags the Security Validation VRT use when tagging Actions include the default SYSTEM account and the User Type values tied to the Action User Profiles. These are:

- **SYSTEM**: the System account on Microsoft(R) Windows(R) operating systems
- **Admin**: An account with Admin privileges
- **Root**: The SuperUser for *nix and macOS operating systems
- **User**: An account with basic, no-admin user, privileges

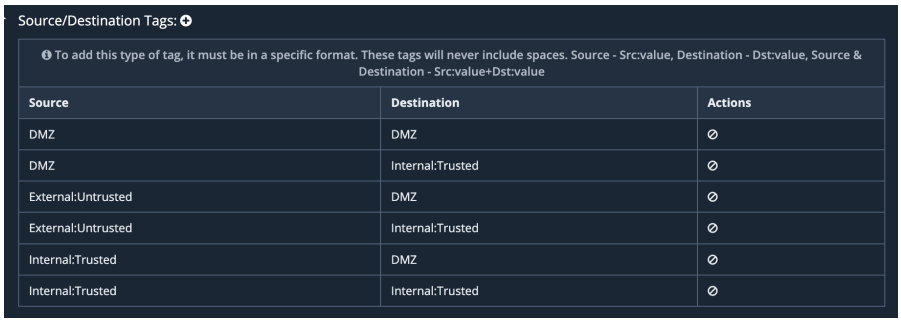
While you can add different tags, these tags are the only four that are considered when running Actions using the Run Recommended option.

(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629cec28e07dc756be50a98d/n/run-as-tags.png)

Run As Tags from two Actions

Source / Destination Tag

Source / Destination Tags suggests the appropriate locations for source and destination Actors. The recommendations the Security Validation VRT includes are based on the Zone attributes for the default Zones configured in your environment. There can be several recommendations, as shown in the following image.



Source and Destination Tags for A100-526

To add this type of tag, use the format described. These tags will never include spaces.

Source:

> **Src:** *VALUE*

Destination:

> **Dst:** *VALUE*

Source & Destination:

> **Src:** *VALUE*+**Dst:** *VALUE*

When you run an Action using the Run Recommended option, the following are the only Source / Destination tags used:

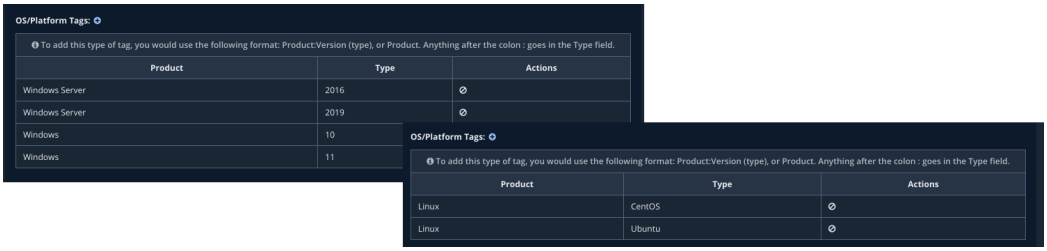
- Src:Internal:Trusted+Dst:External:Untrusted
- Src:Internal:Trusted
- Src:Internal:Trusted+Dst:DMZ
- Src:Internal:Trusted+Dst:Internal:Trusted
- Src:External:Untrusted+Dst:DMZ
- Src:External:Untrusted+Dst:Internal:Trusted
- Src:DMZ+Dst:Internal:Trusted
- Src:DMZ+Dst:DMZ
- Src:DMZ+Dst:External:Untrusted

- Src:External:Untrusted+Dst:External:Untrusted

These tags are created by Security Validation VRT. You can also apply these tags to Actions.

OS / Platform Tags

The OS / Platform tags are straightforward, suggesting which Actors, based on the Actor OS or Platform, the Action can run on. This can be generic, such as **Any**, or specific, such as **Windows 10**.



OS/Platform Tags from 2 Actions

To add this type of tag, use the following format:

```
Product:Version (type)
```

or

```
Product
```

Anything after the colon goes in the Type field.

The OS / Platform tags that are used when you run an Action using the Run Recommended option are:

- Any
- Windows:10
- Windows:11
- Windows Server:2016
- Windows Server:2019
- Linux:CentOS
- Linux:Ubuntu
- macOS

Control Tags

The Control Tags give you a way of knowing which type of security controls the Action tests against. For a full list of Security Validation-provided Control Tags, expand the Controls Dimension filter. You can create the same tags or add your own.