MITRE ATT&CK® DASHBOARD

The MITRE ATT&CK Dashboard lets you identify how well your environment is protected according to MITRE's ATT&CK model (see the **MITRE ATT&CK wiki** **(https://attack.mitre.org)**). The dashboard automatically refreshes every 30 seconds, updating the number of tests completed. For this dashboard to function, Actions must include Security Validation (system) or User Tags to identify which MITRE ATT&CK Tactic, Technique, or Sub-Technique it tests. The majority of Actions provided by Mandiant Advantage Security Validation are tagged with one or more MITRE ATT&CK tags.

The MITRE ATT&CK Tags use the following format:

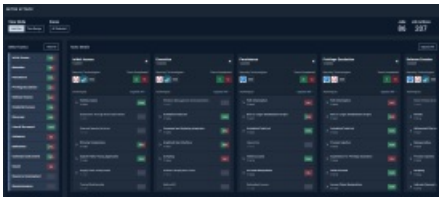
- Tactics: ***ATT&CK:TA####***
- Techniques: ***ATT&CK:T####***
- Sub-Techniques ***ATT&CK:T####.####***

By default, MSV is configured to use the latest MITRE ATT&CK framework that Mandiant supports. To see which versions of the MITRE ATT&CK framework are available and change the setting, if needed, see the **Advanced Settings** **(https://docs.mandiant.com/home/msv-advanced-settings)**.

If you created user tags in a different format, you can update them in the User Tags section of the Tags page. See **Tags** **(https://docs.mandiant.com/home/msv-tags)** for details on the process.

The initial view of the Dashboard shows all Tactics, including respective Techniques, ordered by the lifecycle of adversary behavior. Sub-Techniques are not visible in the initial view, but can be seen when you expand a Technique. Click on a Tactic in the Select Tactics menu to hide or display the Tactic on the Dashboard. Together with the filtering options for View Mode and Zones, you can customize what your MITRE ATT&CK Dashboard displays. See **Filtering the MITRE ATT&CK Dashboard** **(https://docs.mandiant.com/home/filtering-the-mitreattckdashboard)** for more information.

To quickly view the Tactics that matter most to you, click **Hide All** in the Select Tactics menu and then click on the Tactics you want.



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/62880b6b445d5e3e714b3a5f/n/mitre-dashboard.png)

MITRE ATT&CK Dashboard

Viewing Tactic Information

The MITRE ATT&CK Dashboard makes it simple for you to understand how your security technologies are performing against the ATT&CK model. Look at the top of a Tactic's details or find the Tactic under Select Tactics to see an at-a-glance view of your environment's performance.

In a Tactic's Details section, there are two numbers:

- **Green box**: Job Actions that were blocked

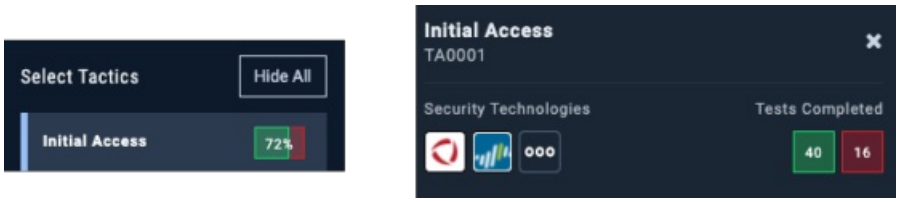
- **Red box**: Job Actions that were not blocked

Together, the counts inside the green and red boxes make up the number of **Tests Completed**. By viewing the numbers under **Tests Completed**, you can easily understand how your environment has performed against that Tactic.

> **NOTE:** These counts include the number of blocked and not blocked Job Actions for that Tactic and its respective Techniques and Sub-Techniques.

> **IMPORTANT:** If the View Mode is set to Last Run, the counts only include the most recent time each Job Action ran. If an Action has a tag added to it but the Action is only included in Jobs that ran in the past, it will not appear in the MITRE dashboard at all.

You can also quickly view the blocked / not blocked statistics for each Tactic under **Select Tactics**, as a percentage. Similar to the green and red boxes under each individual Tactic, the percentage represents the Job Action results related to the Tactic and its Techniques and Sub-Techniques combined.



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/62880b6b445d5e3e714b3a5d/n/blocked-not-blocked-counts.png)

An example of high-level Tactic information in the MITRE Dashbaord

In addition to the blocked / not blocked information provided at the top of each Tactic's details, any security technologies that were observed during the Jobs run for its Techniques and Sub-Techniques are also listed. Moving your cursor over an icon will show you the name of the security technology.

Viewing Techniques and Sub-Techniques in Tactic Details

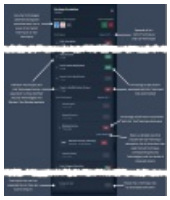
Below each Tactic's security technology icons, you see the Tactic's Techniques and Sub-Techniques. If any Jobs have run for a Technique or Sub-Technique, you will see the percentage of Actions that were blocked.

> **NOTE:** The Techniques and Sub-Techniques listed under each Tactic are the ones that are included as Validation or User tags on one or more of our Actions. We currently have Actions that cover Microsoft(R) Windows(R), Linux, and Apple(R) Macintosh(R) Techniques. Additional Techniques will be included as our Validation Research Team (VRT) adds new Actions.

Techniques and Sub-Techniques can also be expanded, even if they have no related Jobs. When a Technique or Sub-Technique with related Jobs is expanded, you see the security technologies that were seen during the Jobs and counts for the Actions and Job Actions related to it. Each security technology listed, including unknown security technologies, shows the percentage of Job Actions that were blocked. You should keep the following considerations in mind when you review a Technique or Sub-Technique's details:

- A blocked Job Action usually appears for only one security technology, but can appear for multiple security technologies
- If the Job Action wasn't blocked, it may be listed under multiple security technologies

- If the Job Action was blocked but the specific security technology that blocked it couldn't be identified, the Job Action shows as blocked in the unknown security technology category, but could also show as not blocked by one or more security technologies



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/62880b6c445d5e3e714b3a64/n/tactic-explained.png)

Annotated Tactic expanded to show its Techniques and Sub-Techniques

Clicking on **View Details** displays the Technique description and all Jobs that related to that Technique. Here you can work with the Jobs, expanding them to review the individual Job Actions and Events, allowing you to troubleshoot why the Action was not blocked or why a security technology couldn't be identified. It also lets you review how your system performed in the past for each Job Action, but keep in mind that what you see depends on what you've set for the Dashboard's View Mode.

(https://dyzz9obi78pm5.cloudfront.net/app/image/id/62880b6c445d5e3e714b3a66/n/technique-jobs.png)

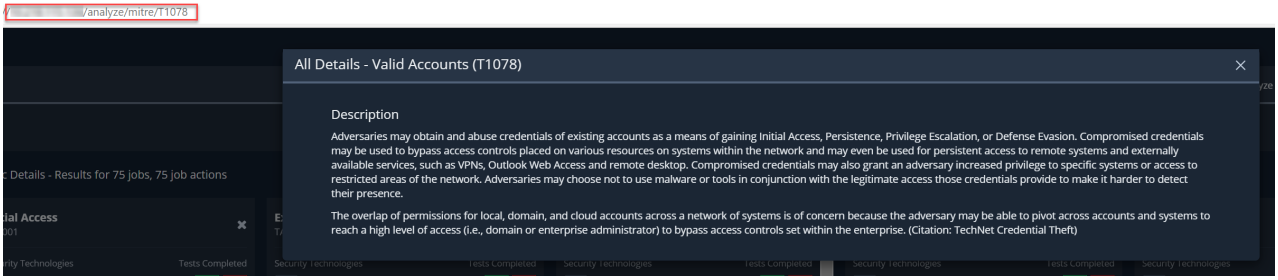
Job Actions for a specific Technique

NOTE: When a Zone filter is applied, the Job list includes Jobs that matched either the source (attacker) or destination (target) Zone.

You can display a specific Technique or Sub-Technique in the MITRE Dashboard by entering its MITRE ID in the URL, using the following format:

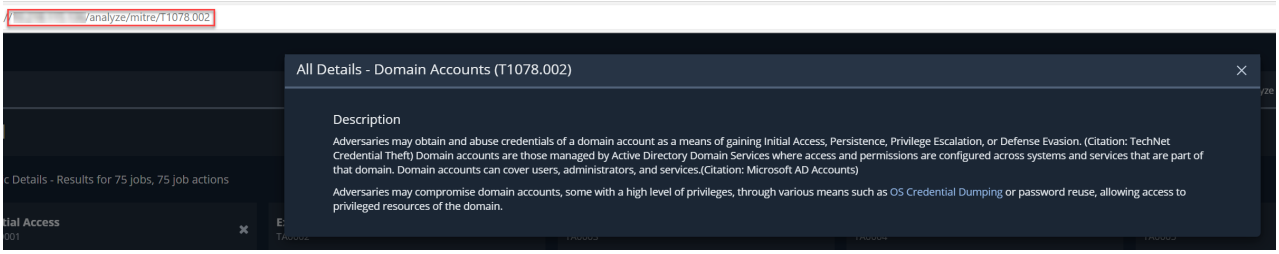
- **/analyze/mitre/T####** (to display Technique details)
- **/analyze/mitre/T####.###** (to display Sub-Technique details)

For example, to automatically display the details for Technique T1078, you would enter /analyze/mitre/T1078 in the URL. The Technique details display, as shown in the following image



Example of URL format to display Technique details

To display Sub-Technique T1078.002, you would enter /analyze/mitre/T1078.002 in the URL, as shown in the following image.



Example of URL format to display Sub-Technique details