SUSPICIOUS EVENTS / MISSING EVENTS

When the Director has an issue correlating an event with a job, it stores it as a Suspicious Event. This can happen for several reasons:

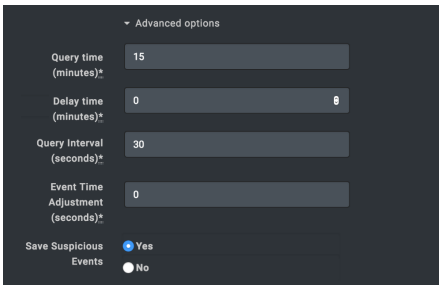
- If the event fails to match the Job's parameters. This occurs when the destination IP is missing.
- If there is an issue with the ports available in the logging.
- If the time of the events drifts from what the Director has observed from the time sources configured at job execution.

Saving Suspicious Events

Allowing Suspicious Events to be saved is a configuration tied to each Integration. By default, this is disabled.

TO SAVE SUSPICIOUS EVENTS

1. Go to **Settings** > **Integrations**.
2. If the Integration already exists, click **Edit**.
   If the Integration is new, click **Add Integration** and select the Integration.
3. Expand **Advanced options**.
4. Scroll to the bottom, and choose **Yes** to save suspicious events.
5. Click **Submit**.
   Suspicious Events are saved and viewable in the platform.



Saving Suspicious Events

Working with Suspicious Events

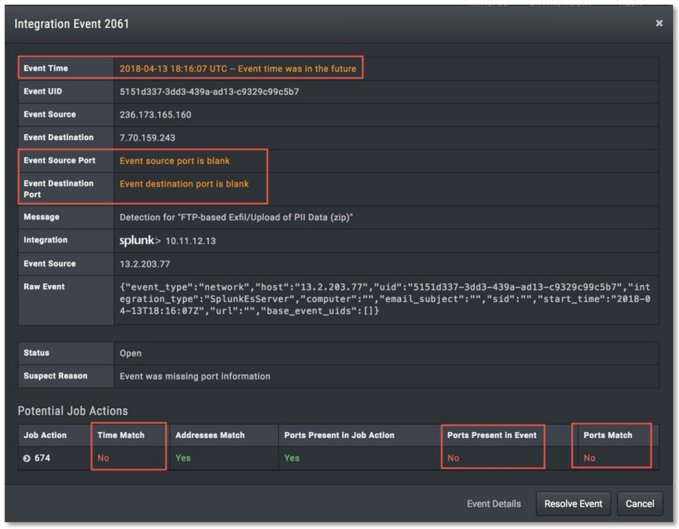
Access the list of suspicious events by:

- Selecting the Jobs menu and choosing **Suspicious events**.
- Selecting a Job from the Process Job Actions page that is part of the Effectiveness Validation Process (EVP).
- Clicking the Suspicious Events icon for an Action on the Job Results page.
- Clicking the Suspicious Event Warning for an Action on the Job Results page.

(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12dcc9cba0017c2f7e06/n/susp-events-missing-1.png)

Clicking **View Event** on a Suspect Integration Event shows the Event details where you can see which fields of the event failed to match the job in two sections.

You can use this information to review the integration details and make or request any required changes.



Integration Event

Once you are satisfied that you have identified the root cause of the failure, click **Resolve event**, and enter information on why you're resolving the event.

When you click **Submit**, the event is removed from the page (but not added to the original job). If you have admin permissions, you can also delete suspect integration events. You can delete all, filtered, or selected events.

IMPORTANT: Deleting events is audited but cannot be reverted.

After the Integration and any other issues have been resolved, rerun the job to verify the changes have resolved the issue and that you aren't seeing the same suspicious events.

Deleting Suspicious Events

The Validation Platform can be configured to automatically remove old Suspicious Events. This helps free up disk space and is more efficient than removing them from the Suspicious Events page.

TO DELETE OLD SUSPICIOUS EVENTS:

1. Go to **Settings** > **Director Settings**.
2. Select **Integrations**.
3. Select **Yes** for Delete old Suspicious Events
4. Enter the number of days they should be kept and click **Update Integration Settings**.

NOTE: At minimum, you must keep them for a day.