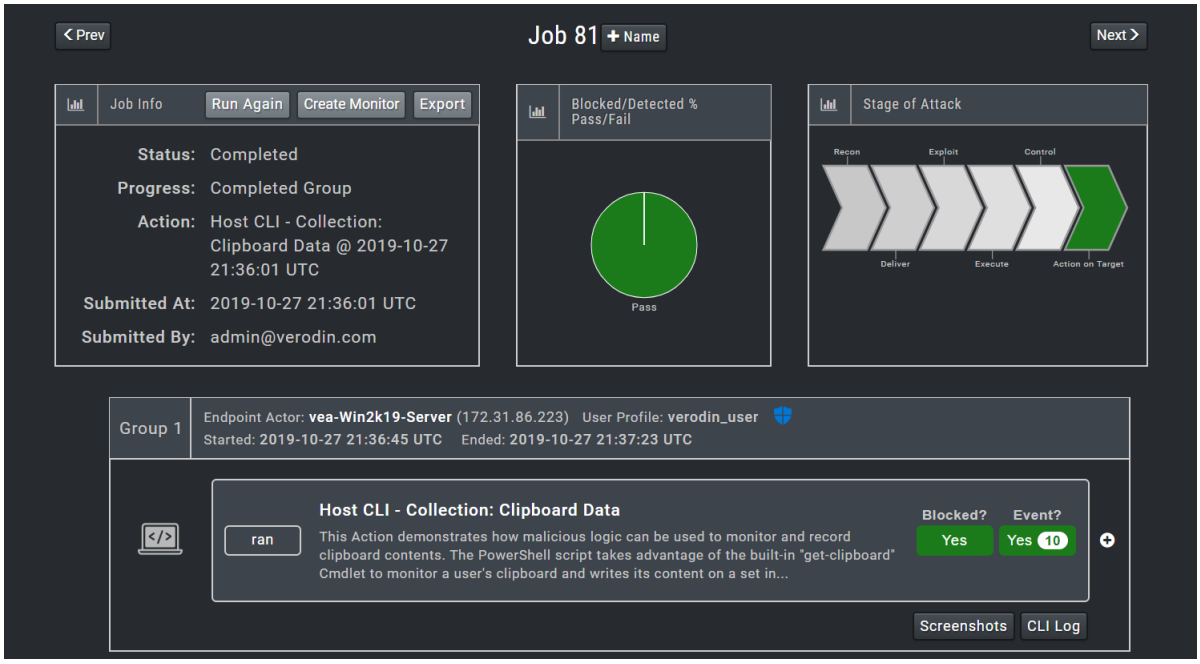
UNDERSTANDING JOB RESULTS - CLASSIC VIEW

NOTE: This was the standard Job Results view through version 4.2.2.0.

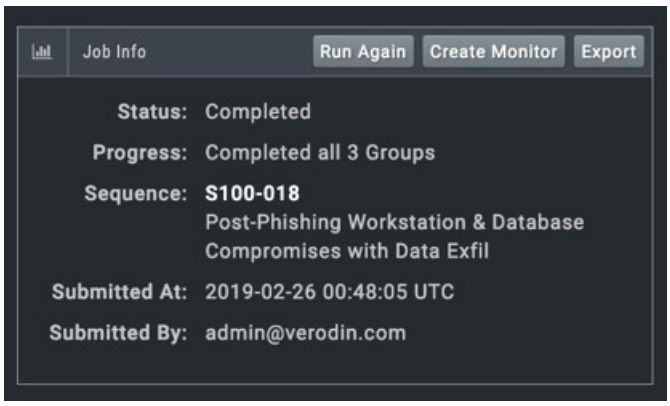
This section provides an overview of the information contained in the Job's page to help you understand your results.



Job's page

When reviewing the results for a particular Job, pay attention to these key areas:

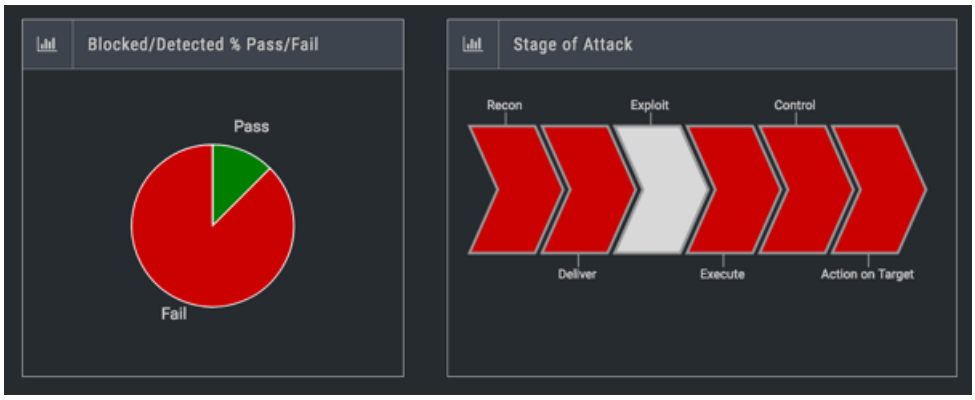
- The Job Info pane shows the Job status, progress, the name of the Action/Sequence/Evaluation/Monitor (also includes VID and security content type if it is a Sequence or Evaluation) processed, the Job submittal time, and the originating user.



Job Info pane

- The pie chart and Stage of Attack arrow chart provide high-level information on the "Passed" and "Failed" Actions

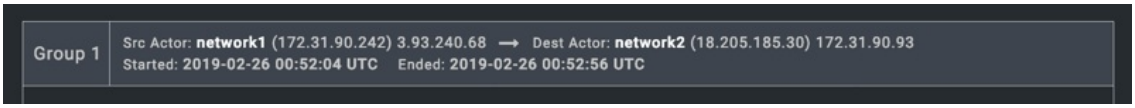
(refer to **Pass/Fail Rules** (https://docs.mandiant.com/home/msv-passfail-rules), for more information).



Job pie chart and Stages of Attack

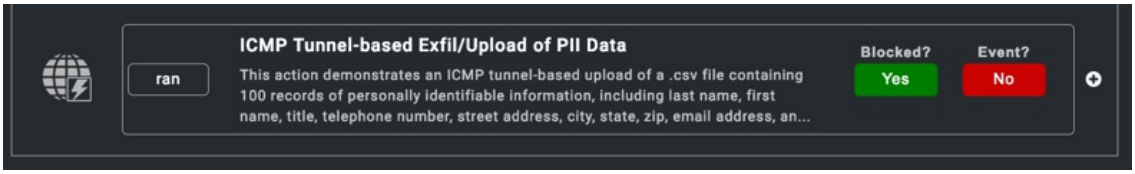
- Each Group contains one or more Actions. The Group heading includes the Actor information, the language if it's not English, and the start and end time, which may differ from the Job Submitted time.

> **NOTE:** If you are watching the results populate as the Job runs, you may notice the source and destination addresses update at the end of the Job. When an Action is running, the Validation Platform only knows the ActorInterface addresses. The platform might also know the destination address that the source needs to use, such as when an AWS Actor is behind a NAT in AWS so its NIC IP is different from the external IP you use to reach it. In cases where the source Actor is going through a NAT, the platform doesn't know the external address of that NAT until the destination Actor sees it and returns its info upon completing the Job Action.



Jobs Group heading

- Each Action has a separate row that includes or may include:



Job Action details

  - A cell for Blocked? which includes either Yes or No, thus identifying blocking behaviors by defenses
  - A cell for Event? which includes either Yes (#) or No, thus identifying how many detection events related to that Action's execution were logged
  - A question mark, if events were logged that might match the Action but could not be 100% related. When an event cannot be matched to a Job Action, a Suspicious Event is logged.
  - A plus sign button from which a Monitor may be created (refer to **Monitors / Advanced Environmental Drift Analysis (AEDA)** (https://docs.mandiant.com/home/monitors-advanced-environmental-drift-analysis-aeda) for more information)

> **NOTE:** If a Job Action has been disabled, the plus sign used to create a monitor does not appear for that Action.

- A magnifying glass to view the Action logs, when they are available

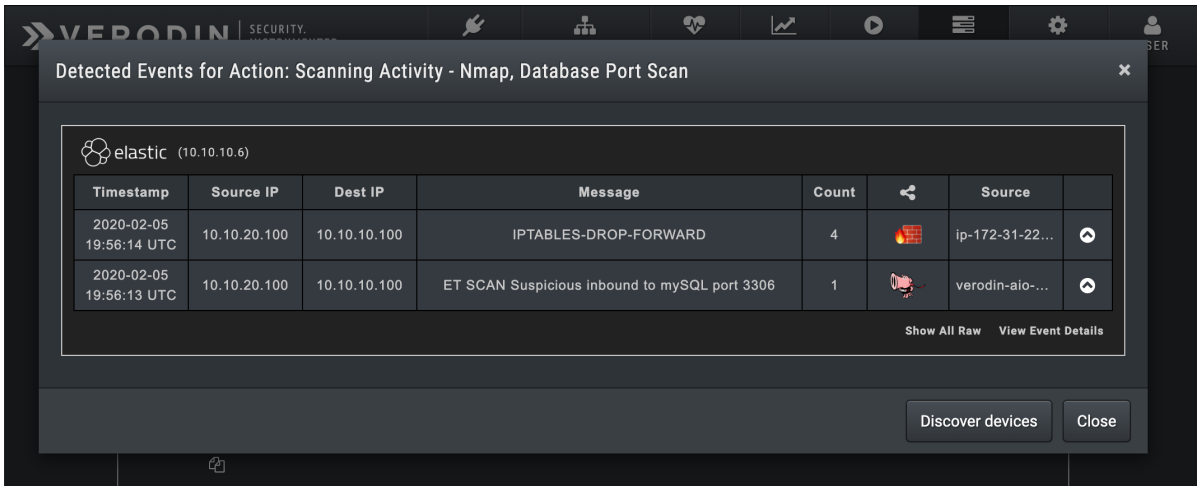
  > **NOTE:** The magnifying glass will only appear if you have enabled Show Debug Links for Jobs (option is listed in User Preferences, access by going to **User** > **User Preferences** or if ?debug is added to the end of the job results url.

- An info icon that displays the proxy used, when applicable
- A clickable triangle to indicate if there was a Block HTTP page that came up and if there is a Block rule in place for that page. The triangle is yellow if no block rule, white if there is a block rule.
- A CLI Log button for Host CLI Actions
- A Screenshots button for Host CLI Actions run on Protected Theater

  > **NOTE:** Actions that are run as System or use Bash Shell do not have screenshots.

- An edit icon that opens the edit Action form (for user-created Actions)
- A clone icon that clones the Action

When the Event cell shows Yes, clicking on it displays event information, grouped by Integration.

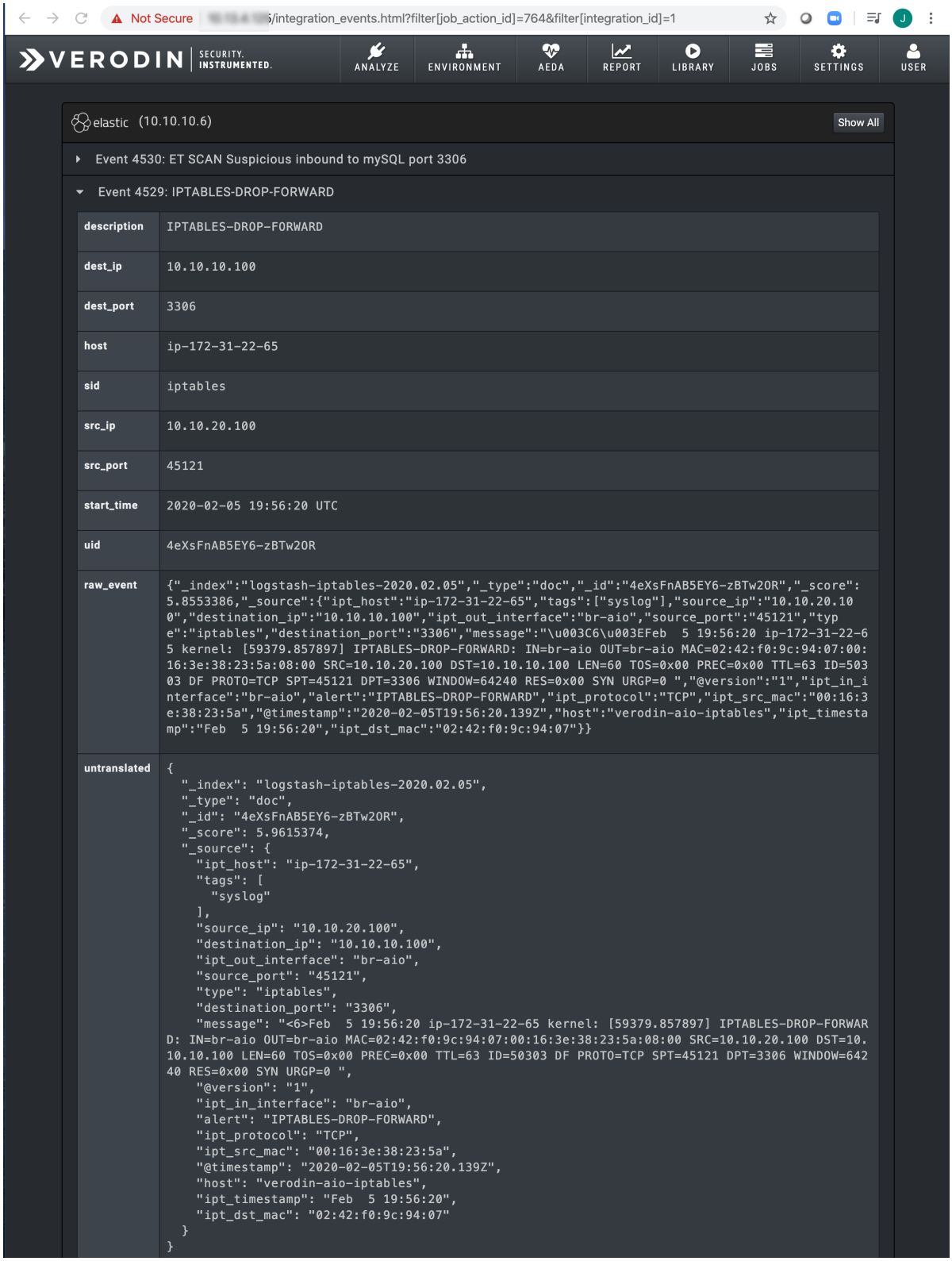


Detection Events for a Job

The information displayed includes:

- The timestamp
- Source and destination IP addresses
- The event Message(s)
- The count/number of events of that combination
- The security technology associated with the event (or an add security technology icon)
  You can click on the security technology icon or the add security technology icon to open the Create/View Security Technology form. This form displays all information on that event, shows any existing definitions used to identify the security technology, and allows you to add new definitions. Adding definitions is part of the Effectiveness Validation Process (EVP).
- The Source of the event (IDS, IPS, DLP, etc.).

You can expand each event to see the Raw data or click **Show All Raw** to display all raw events under the table. Clicking **View Event Details** takes you to a new page that displays the complete attributes for the event, including the raw response the Validation Platform received from the Integration's API.



Integration Event details page