VIEW EVENTS

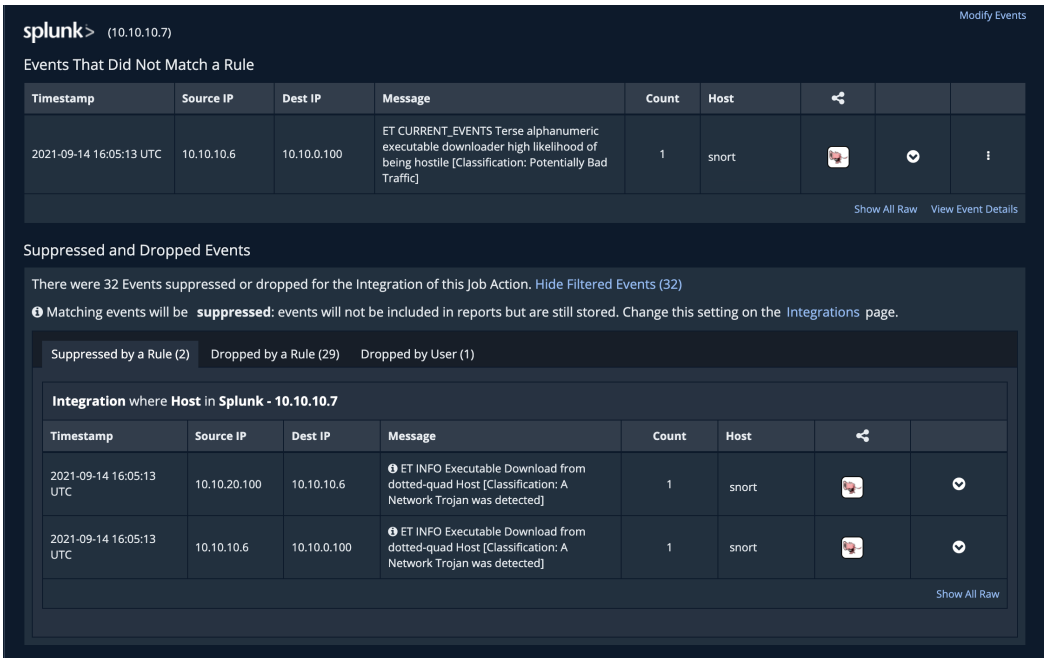
Each Job Action that was Detected should have events associated with it, as long as you've setup one or more integrations or have a security technology on an Endpoint Actor. The information contained in each event is determined by the Integration. You can view a Job's Events from the Job Status page and from the Job Details page. When the Events section for a Job Action is open, you see sections for each Integration that detected the event. If you're on the Job Details page and there are one or more events generated, you also see the Modify Events option above all tables (see **Reassigning, Suppressing, and Dropping Events (https://docs.mandiant.com/home/reassigning-suppressing-and-dropping-events)** for more information).

These tables display the following details for the events:

- The timestamp
- Source and destination IP addresses
- The event Message(s)
- The count/number of events of that combination
- The Host / Source of the event (IDS, IPS, DLP, etc.)
- The security technology associated with the event (or an add security technology icon)

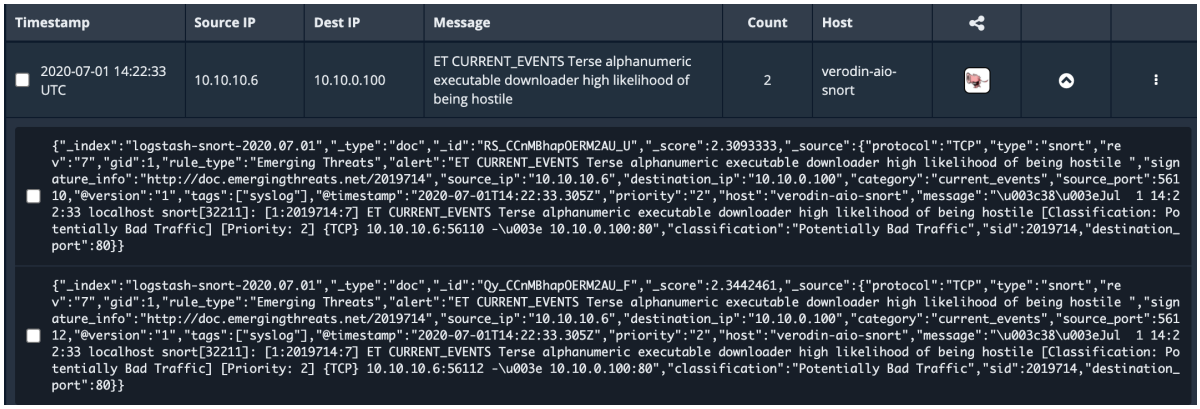
> **NOTE:** You can click on the security technology icon or the add security technology icon to open the Create/View Security Technology form. This form displays all information on that event, shows any existing definitions used to identify the security technology, and allows you to add new definitions. Adding definitions is part of the Effectiveness Validation Process (EVP).

If events have been suppressed or dropped by an Event Filter Rule or manually by a user, you'll also see a Suppressed and Dropped Events section. This section can be expanded to see additional details on the suppressed and dropped events.



Job Action's Event section expanded

In the overview, you can expand an event to see additional fields and details that were captured.



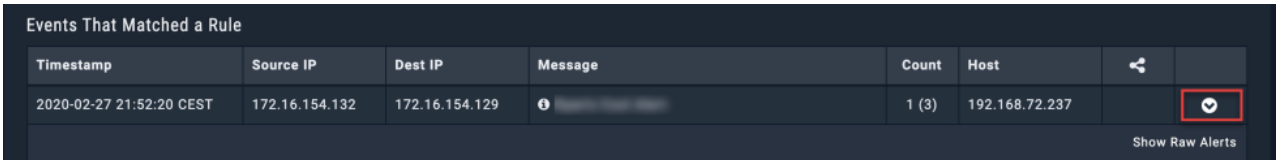
Raw Events for a Job

How Correlation Rules Affect Events

When events trigger a correlation rule in an integration, an alert is generated. If the integration supports correlation rules, you may see two tables for the events: Events That Matched a Rule and Events That Didn't Match a Rule.

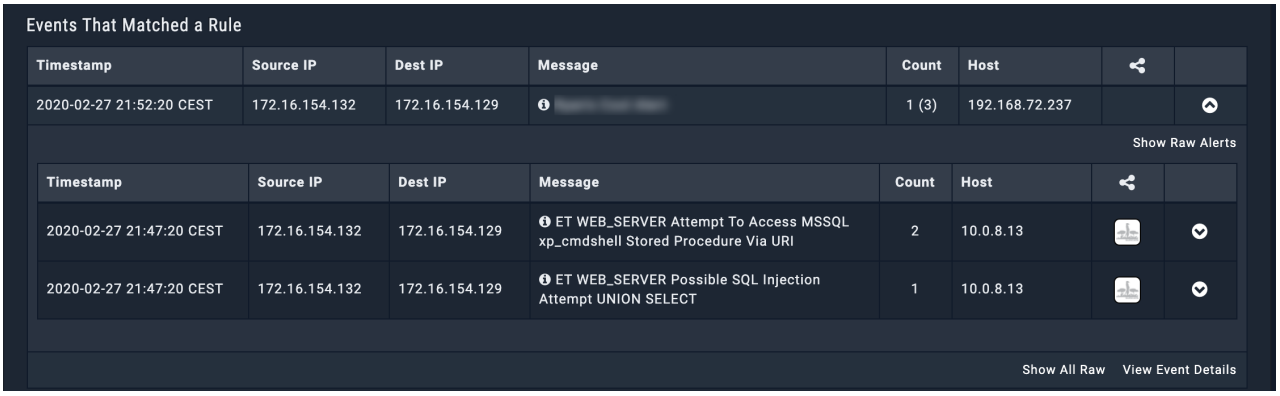
> **NOTE:** OS-specific security technologies such as Windows Defender may include slightly different information.

Security Validation associates alerts with their base events and displays them in the Events That Matched a Rule table. To understand how many events are associated with an alert, look at the Count column in the table. The count shows both the number of alerts and the number of related events in the same column. For example, if an alert count shows 1 (3), it means that a single alert has three events associated with it.



Events That Matched a Rule - One alert with three related events

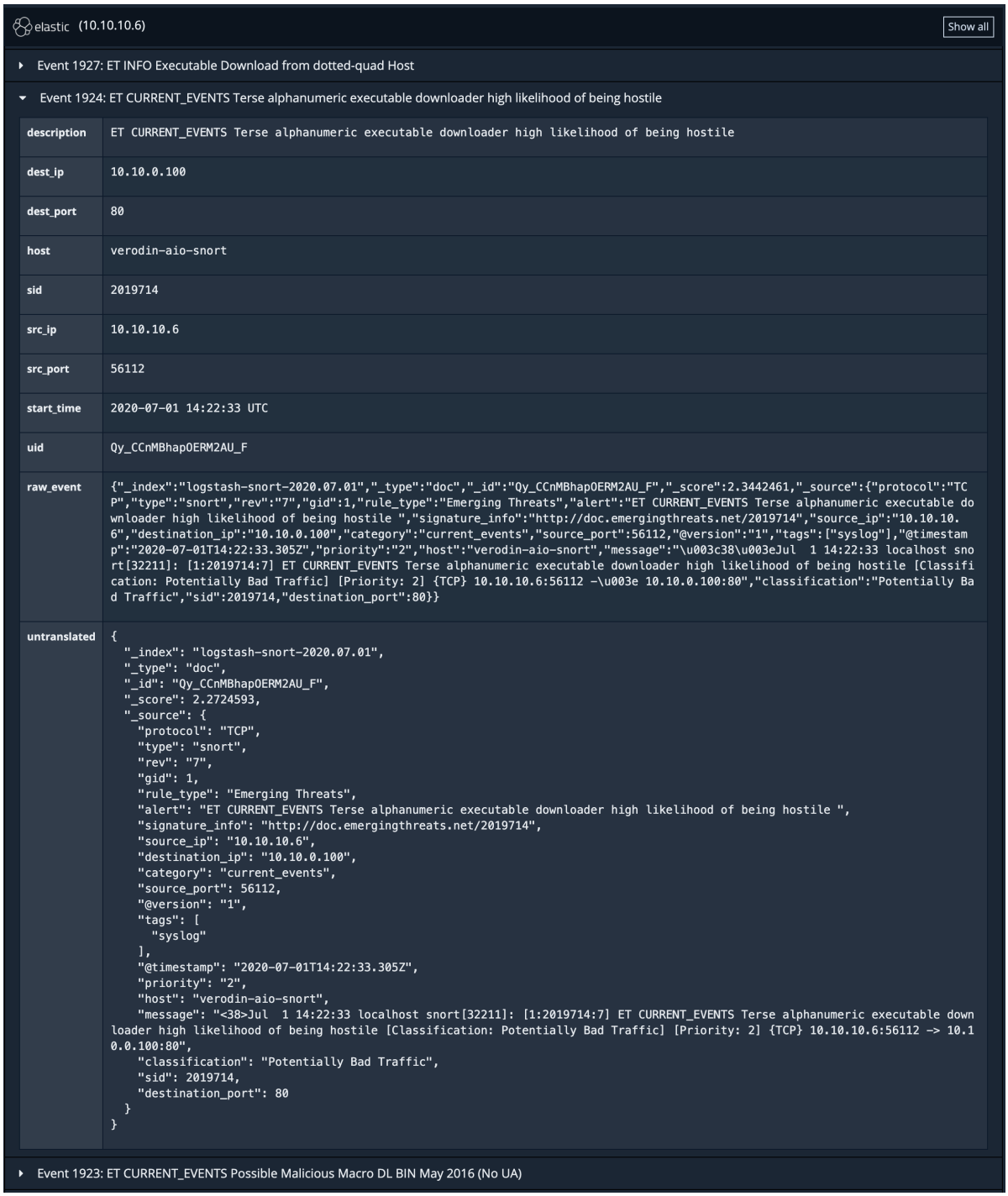
Events associated with alerts are nested inside the Events That Matched a Rule table, but can be viewed by selecting expand.



Events That Matched a Rule - One alert with three related events, expanded

Raw Event Details

Depending on the operating system, an event may include an expand/collapse button that allows you to view the raw details for the event. You can also click **Show All Raw** to expand all events in the table. Clicking **View Event Details** opens a new page that displays the complete attributes for the event, including the raw response Validation Platform received from the Integration's API.



Integration Event details page