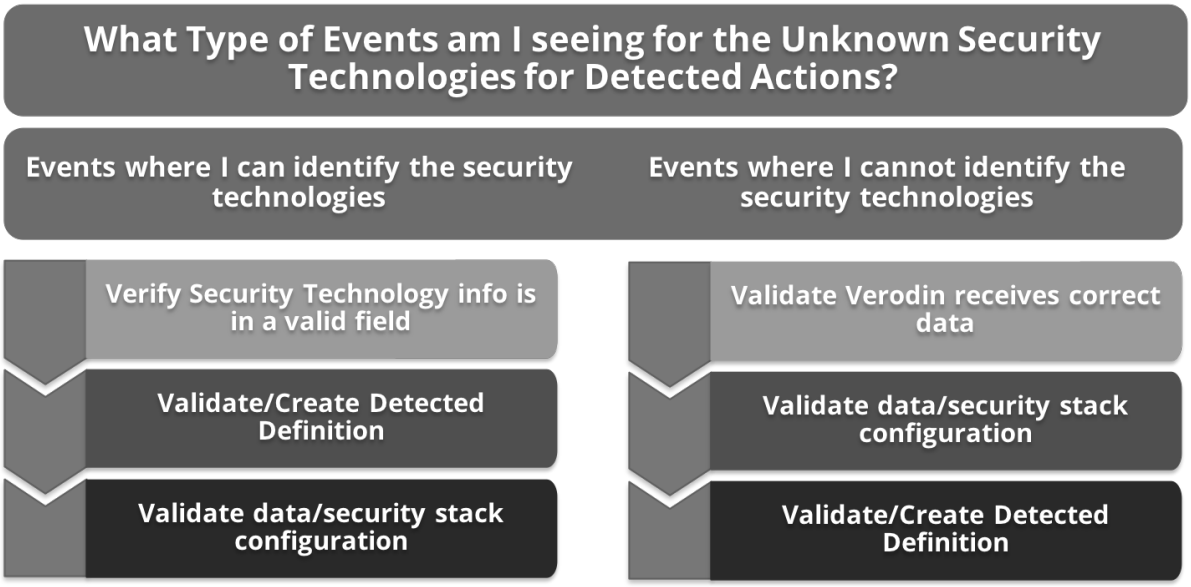
WORKING WITH UNCATEGORIZED DETECTED ACTIONS

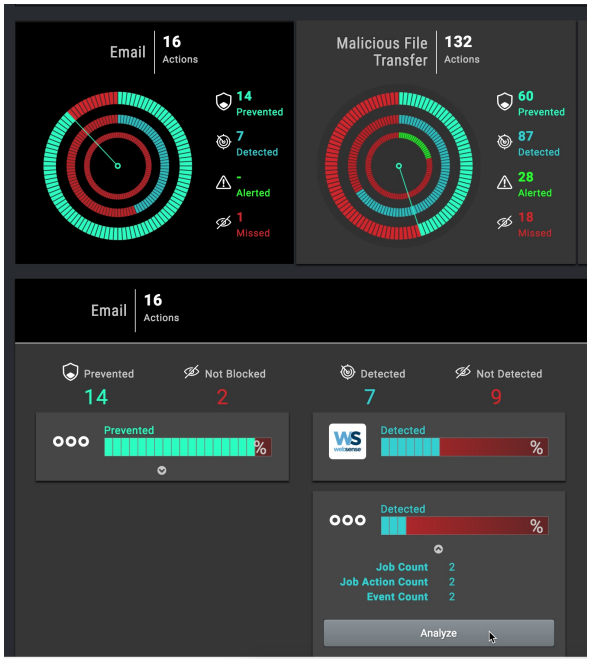
Now that you have a list of Actions that are not associated with specific security technologies, you need to identify why this has occurred and resolve any issues so you can strengthen the security posture of your network. To do this, review the Job Actions and Events to determine the best route forward. To illustrate the process, the following sections contain use cases that you might encounter and provides the mitigation steps to resolve the issues.

IMPORTANT: When you add or edit security technology definition and prevention information, the changes have to be processed, so the updates to the Jobs, Events, and Gauges may not display immediately.



Workflow for Resolving Detected Unknown Security Technologies Actions

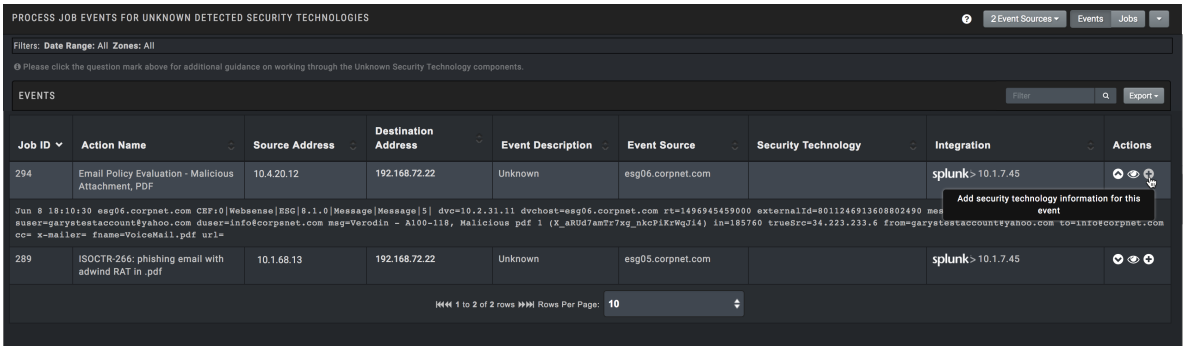
Security Technology Information Available in the Events



Email Unknown Detected Gauge Details

Consider this Email Gauge. A little under half of the Attacks were detected, with some related to WebSense and some that are not related to a security technology.

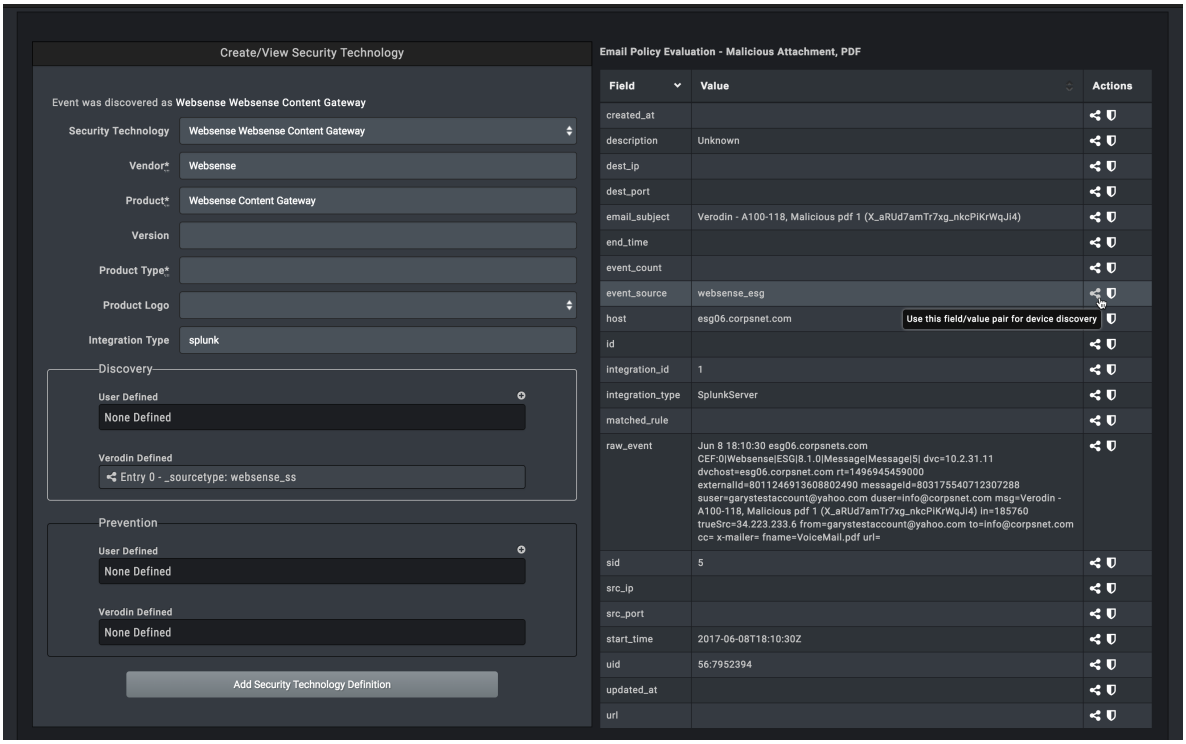
Clicking **Analyze** opens a new page that displays the Events included in the uncategorized Email Attack Actions. You can work from this view, which allows you to view the raw event data and jump to the Job page. Or, you can switch over to the Jobs View and review the Actions individually. Start your troubleshooting from the Events page by expanding the first event to see the raw data. Right away, you see the raw data includes Websense, so you are able to identify the security technology. Now that you have identified a security technology, you want to see if the Validation Platform has any additional information about the event and potentially create a new security technology, so you click **Add Security Technology**.



Process Job Events for Unknown Detected Security Technologies - Email Attacks

On this page you see the raw Event data as well as all the other fields that the platform received data for, including the event_source field. Since the event_source field is populated, this is an instance where you need to add a user-defined security technology because the default definition does not include the specific value that is displayed. Select

Websense/Forcepoint Websense Firewall from the Security Technology list, verify that all the required fields are populated and display the Validation Platform definitions. After verifying the existing definitions do not include the value in event_source, click **Add to Discovery** definition next to the event_source field. This populates the User Defined Discovery field.



Security Technology Definition for Websense - no User-defined definitions

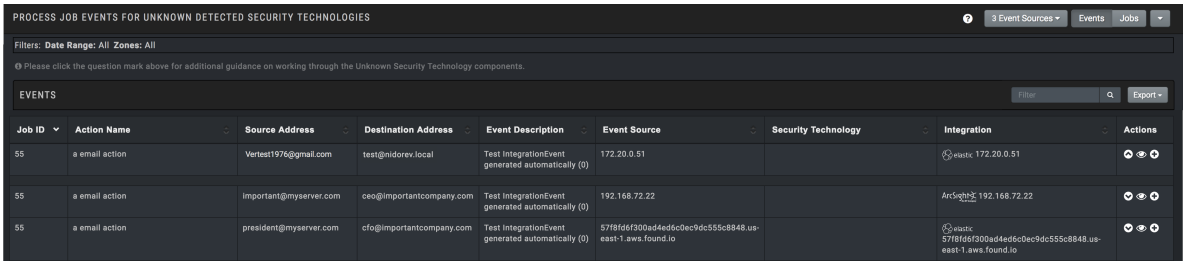
When you click **Add Security Technology Definition**, the changes are saved and the Validation Platform runs through the unknown events in the system and assigns the technology where appropriate. A flash card displays, informing you how many matches were found. This message can also be seen by going into your messages section. The platform also automatically applies the definition to future events.

IMPORTANT: If Websense had only appeared in the raw_event field, adding the Security Technology definition would not have been the primary remediation step. Not having the security technology information in its own field, the security of your network could be negatively impacted, potentially leading to missed alerts.

Once you have tuned your network and verified Websense is populating correctly, thus allowing the integration to properly identify the security technology, you could temporarily add a security definition using the instance of Websense in the raw event data field to have the Validation Platform assign the technology to the Events. However, once the events were related to Websense, you would want to remove the definition. This way, you would be aware if the issue reappears in the future.

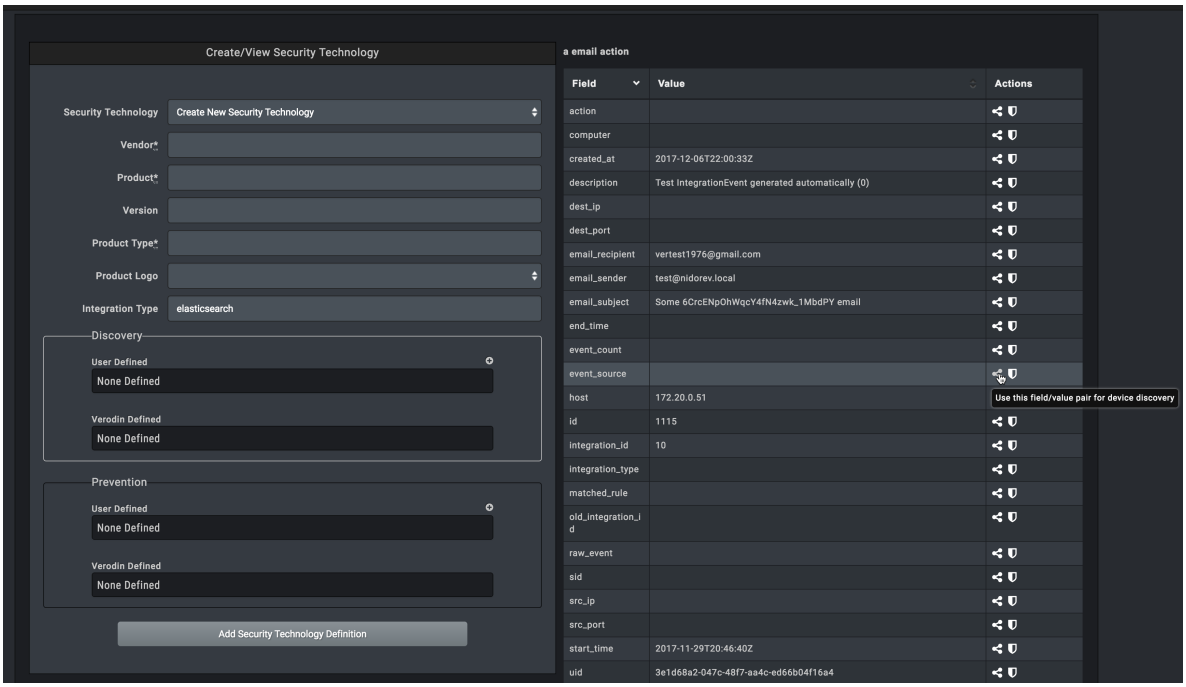
No Security Technology Information Available

As you are working through the unknown security technology category for your Detected Actions, you try to view the raw data for the first event listed and find there is not any.



Processed Job Events for Detected Actions

To search for additional context, click Add New Security Technology (⊕) to see all the data the Validation Platform has for the event.



The Create/View Security Technology Form showing Event info

Based on your understanding of the network, you may recognize which security technology the event comes from. However, just looking at the event details on the security technology form in the platform, you cannot, and thus do not add a Security Technology definition. Instead you proceed to tune your security stack to resolve the issue. Once you have tuned your security stack, rerun the Job to see if the security technology is now recognized, and if it is not, if the events have enough information to allow you to add the security technology definition.

It can be difficult to clear out the unknown security technology Actions when the events do not have the necessary information to identify the security technology. After addressing the root cause of the issue in your security stack and rerunning the Job to verify all events are related to a security technology, you could choose to delete the entire Job, keep the Job, knowing that it will continue to show up as uncategorized for the Detected Actions, or potentially add a temporary security technology definition to associate the events to the appropriate security technology.

If you do decide to add a temporary security technology definition, identify something that is unique to the event. If you

do not, you may build an inaccurate relationship between those events and an unrelated security technology. If this happens, the only way to remove that relationship is to delete the Security Technology from the Environment page. When you do this, all Actions and events related to that Security Technology would be automatically updated to remove the Security Technology information. After the Security Technology is deleted you would rediscover it by modifying the Security Technology definition.