

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) (<https://docs.mandiant.com/home/reassigning-suppressing-and-dropping-events>) for more information).

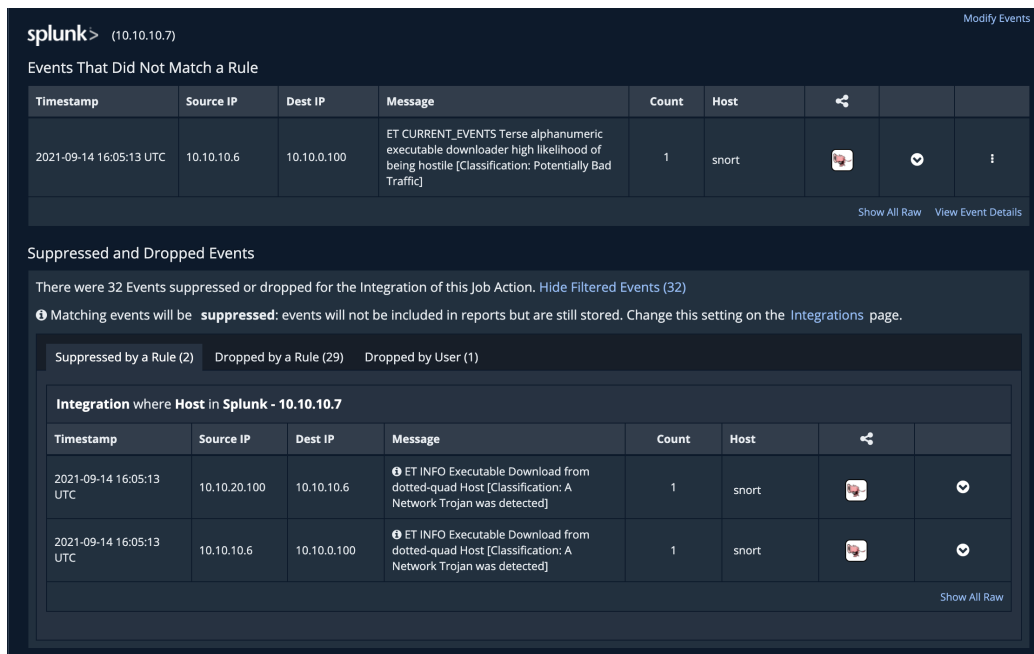
These tables display the following details for the events:

- 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.



The screenshot shows the Splunk interface for a job action. At the top, it says 'splunk> (10.10.10.7)' and 'Modify Events'. Below that, there's a section titled 'Events That Did Not Match a Rule' with a table containing one event:

Timestamp	Source IP	Dest IP	Message	Count	Host			
2021-09-14 16:05:13 UTC	10.10.10.6	10.10.0.100	ET CURRENT_EVENTS Terse alphanumeric executable downloader high likelihood of being hostile [Classification: Potentially Bad Traffic]	1	snort			




Below this table are links for 'Show All Raw' and 'View Event Details'. The next section is 'Suppressed and Dropped Events', which states 'There were 32 Events suppressed or dropped for the Integration of this Job Action. Hide Filtered Events (32)'. It includes a note: 'Matching events will be suppressed: events will not be included in reports but are still stored. Change this setting on the Integrations page.' There are three sub-sections: 'Suppressed by a Rule (2)', 'Dropped by a Rule (29)', and 'Dropped by User (1)'. The 'Suppressed by a Rule (2)' section is expanded, showing a table for 'Integration where Host in Splunk - 10.10.10.7':

Timestamp	Source IP	Dest IP	Message	Count	Host		
2021-09-14 16:05:13 UTC	10.10.20.100	10.10.10.6	 ET INFO Executable Download from dotted-quad Host [Classification: A Network Trojan was detected]	1	snort		
2021-09-14 16:05:13 UTC	10.10.10.6	10.10.0.100	 ET INFO Executable Download from dotted-quad Host [Classification: A Network Trojan was detected]	1	snort		

At the bottom of this section is a link for 'Show All Raw'.

Job Action's Event section expanded

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

Timestamp	Source IP	Dest IP	Message	Count	Host			
2020-07-01 14:22:33 UTC	10.10.10.6	10.10.0.100	ET CURRENT_EVENTS Terse alphanumeric executable downloader high likelihood of being hostile	2	verodin-aio-snort			

```

{"_index":"logstash-snort-2020.07.01","_type":"doc","_id":"RS_CCrMBhap0ERM2AU_U","_score":2.3093333,"_source":{"protocol":"TCP","type":"snort","rev":"7","gid":1,"rule_type":"Emerging Threats","alert":"ET CURRENT_EVENTS Terse alphanumeric executable downloader high likelihood of being hostile","signature_info":"http://doc.emergingthreats.net/2019714","source_ip":"10.10.10.6","destination_ip":"10.10.0.100","category":"current_events","source_port":56110,"version":"1","tags":["syslog"],"@timestamp":"2020-07-01T14:22:33.305Z","priority":"2","host":"verodin-aio-snort","message":"\u003c38\u003eJul 1 14:22:33 localhost snort[32211]: [1:2019714:7] ET CURRENT_EVENTS Terse alphanumeric executable downloader high likelihood of being hostile [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 10.10.10.6:56110 -\u003e 10.10.0.100:80","classification":"Potentially Bad Traffic","sid":2019714,"destination_port":80}}
    
```

```

{"_index":"logstash-snort-2020.07.01","_type":"doc","_id":"Qy_CCrMBhap0ERM2AU_F","_score":2.3442461,"_source":{"protocol":"TCP","type":"snort","rev":"7","gid":1,"rule_type":"Emerging Threats","alert":"ET CURRENT_EVENTS Terse alphanumeric executable downloader high likelihood of being hostile","signature_info":"http://doc.emergingthreats.net/2019714","source_ip":"10.10.10.6","destination_ip":"10.10.0.100","category":"current_events","source_port":56112,"version":"1","tags":["syslog"],"@timestamp":"2020-07-01T14:22:33.305Z","priority":"2","host":"verodin-aio-snort","message":"\u003c38\u003eJul 1 14:22:33 localhost snort[32211]: [1:2019714:7] ET CURRENT_EVENTS Terse alphanumeric executable downloader high likelihood of being hostile [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 10.10.10.6:56112 -\u003e 10.10.0.100:80","classification":"Potentially Bad Traffic","sid":2019714,"destination_port":80}}
    
```

Raw Events for a Job

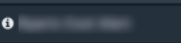



How Correlation Rules Affect Events

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								
Timestamp	Source IP	Dest IP	Message	Count	Host			
2020-02-27 21:52:20 CEST	172.16.154.132	172.16.154.129		1 (3)	192.168.72.237			

Show Raw Alerts

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

Timestamp	Source IP	Dest IP	Message	Count	Host		
2020-02-27 21:52:20 CEST	172.16.154.132	172.16.154.129	[REDACTED]	1 (3)	192.168.72.237		
Show Raw Alerts							
Timestamp	Source IP	Dest IP	Message	Count	Host		
2020-02-27 21:47:20 CEST	172.16.154.132	172.16.154.129	ET WEB_SERVER Attempt To Access MSSQL xp_cmdshell Stored Procedure Via URI	2	10.0.8.13		
2020-02-27 21:47:20 CEST	172.16.154.132	172.16.154.129	ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT	1	10.0.8.13		
Show All Raw View Event Details							

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.

elastic (10.10.10.6)
Show all

- ▶ Event 1927: ET INFO Executable Download from dotted-quad Host
- ▼ Event 1924: ET CURRENT_EVENTS Terse alphanumeric executable downloader high likelihood of being hostile

description	ET CURRENT_EVENTS Terse alphanumeric executable downloader high likelihood of being hostile
dest_ip	10.10.0.100
dest_port	80
host	verodin-ai0-snort
sid	2019714
src_ip	10.10.10.6
src_port	56112
start_time	2020-07-01 14:22:33 UTC
uid	Qy_CcNMBhap0ERM2AU_F
raw_event	<pre>{ "_index": "logstash-snort-2020.07.01", "_type": "doc", "_id": "Qy_CcNMBhap0ERM2AU_F", "_score": 2.3442461, "_source": { "protocol": "TCP", "type": "snort", "rev": "7", "gid": 1, "rule_type": "Emerging Threats", "alert": "ET CURRENT_EVENTS Terse alphanumeric executable downloader high likelihood of being hostile", "signature_info": "http://doc.emergingthreats.net/2019714", "source_ip": "10.10.10.6", "destination_ip": "10.10.0.100", "category": "current_events", "source_port": 56112, "@version": "1", "tags": ["syslog"], "@timestamp": "2020-07-01T14:22:33.305Z", "priority": "2", "host": "verodin-ai0-snort", "message": "\u003c38\u003eJul 1 14:22:33 localhost snort[32211]: [1:2019714:7] ET CURRENT_EVENTS Terse alphanumeric executable downloader high likelihood of being hostile [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 10.10.10.6:56112 -> \u003c38\u003e 10.10.0.100:80", "classification": "Potentially Bad Traffic", "sid": "2019714", "destination_port": "80"}}</pre>
untranslated	<pre>{ "_index": "logstash-snort-2020.07.01", "_type": "doc", "_id": "Qy_CcNMBhap0ERM2AU_F", "_score": 2.2724593, "_source": { "protocol": "TCP", "type": "snort", "rev": "7", "gid": 1, "rule_type": "Emerging Threats", "alert": "ET CURRENT_EVENTS Terse alphanumeric executable downloader high likelihood of being hostile", "signature_info": "http://doc.emergingthreats.net/2019714", "source_ip": "10.10.10.6", "destination_ip": "10.10.0.100", "category": "current_events", "source_port": 56112, "@version": "1", "tags": ["syslog"], "@timestamp": "2020-07-01T14:22:33.305Z", "priority": "2", "host": "verodin-ai0-snort", "message": "<38>Jul 1 14:22:33 localhost snort[32211]: [1:2019714:7] ET CURRENT_EVENTS Terse alphanumeric executable downloader high likelihood of being hostile [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 10.10.10.6:56112 -> 10.10.0.100:80", "classification": "Potentially Bad Traffic", "sid": "2019714", "destination_port": "80" } }</pre>

- ▶ Event 1923: ET CURRENT_EVENTS Possible Malicious Macro DL BIN May 2016 (No UA)

Integration Event details page