Splunk® App for PCI Compliance
Installation and Configuration Manual 4.0.0

Notable events

Generated: 1/16/2020 4:40 am
Notable events

When a **correlation search** included in the Splunk App for PCI Compliance (or added by a user) identifies an event or pattern of events, it creates a notable event. Correlation searches filter the IT security data and correlate across events to identify a particular type of incident (or pattern of events) and then create **notable events**. The app includes pre-configured correlation searches to create notable events, and lets you add your own.

Correlation searches run at regular intervals (for example, every hour) or continuously in real-time and search events for a particular pattern or type of activity. The notable event is stored in a dedicated notable index, which is implemented as a summary index in Splunk Enterprise. The **Incident Review** dashboard is used to view and act on notable events. A notable event might be a single event of high importance, such as any activity from a known web attacker, or an aggregate of multiple events that together warrant review, such as a high number of authentication failures on a single host followed by a successful authentication.

When notable events are created, relevant information from the asset list is combined with the event information. To help to further identify important patterns, correlation searches are each assigned a "severity" of informational, low, medium, high, or critical. Notable events are assigned an "urgency", based on the severity of the event and the priority of the asset corresponding to the event.

<table>
<thead>
<tr>
<th>Asset Priority</th>
<th>Event Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown</td>
<td>Informational</td>
</tr>
<tr>
<td>Low</td>
<td>Informational</td>
</tr>
<tr>
<td>Medium</td>
<td>Informational</td>
</tr>
<tr>
<td>High</td>
<td>Informational</td>
</tr>
<tr>
<td>Critical</td>
<td>Informational</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Event Severity</th>
<th>Informational</th>
<th>Unknown</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
<th>Critical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Informational</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>Critical</td>
</tr>
<tr>
<td>Unknown</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>Critical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>Critical</td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>Critical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>Critical</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Critical</td>
<td>Medium</td>
<td>High</td>
<td>Critical</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- If event severity is informational, the event urgency is informational, regardless of asset priority.
- If asset priority is unknown or low and event severity is unknown, low, or medium, the event urgency is low.
- If asset priority is unknown or low and event severity is high, the event urgency is medium.
- If asset priority is unknown or low and event severity is critical, the event urgency is high.
- If asset priority is unknown or low and event severity is critical, the event urgency is high.
• If asset priority is medium and event severity is unknown or low, the event urgency is low.
• If asset priority is medium and event severity is medium, the event urgency is medium.
• If asset priority is medium and event severity is high, the event urgency is high.
• If asset priority is medium and event severity is critical, the event urgency is critical.
• If asset priority is high and event severity is unknown, low, or medium, the event urgency is medium.
• If asset priority is medium and event severity is high, the event urgency is high.
• If asset priority is medium and event severity is critical, the event urgency is critical.
• If asset priority is critical and event severity is unknown or low, the event urgency is medium.
• If asset priority is critical and event severity is medium, the event urgency is high.
• If asset priority is critical and event severity is high or critical, the event urgency is critical.

Correlation searches do not use the calculated severity described if the events being searched contain a severity field.

How to suppress notable events

In some cases, you might want to prevent certain types of notable events from appearing on the Incident Review dashboard or contributing to alert thresholds. To do this, you need to create a notable event suppression. See Suppressing notable events in this manual.

Manually create a notable event

You can manually create a notable event from an indexed event, or create one from scratch.

Note: By default, only administrators can manually create notable events. To grant other users this capability, see Configure user and roles in the Installation and Upgrade Manual.
Create a notable event from an existing event

You can create a notable event from any indexed event using the Event Actions menu. Do not create a notable event from notable events on the Incident Review dashboard.

1. From an event, view the event details and click Event Actions.
2. Select Create notable event.
3. Enter a Title for the event.
4. (Optional) Select a security Domain.
5. (Optional) Select an Urgency level.
6. (Optional) Select an Owner.
7. (Optional) Select a Status.
8. Enter a Description for the event that describes why you created the notable event or what needs to be investigated.
9. Save the new notable event. The Incident Review dashboard displays with your new notable event.

Note: A notable event created in this way includes tracking fields such as Owner and Status, but does not include the unique fields or links created when a notable event is generated by a correlation search alert action.

Create a notable event from scratch

Create a notable event based on observations, a finding from a security system outside Splunk software, or something else.

1. Select Configure > Incident Management > New Notable Event.
2. Enter a Title for the event.
3. (Optional) Select a security Domain.
4. (Optional) Select an Urgency level.
5. (Optional) Select an Owner.
6. (Optional) Select a Status.
7. Enter a Description for the event that describes why you created the notable event or what needs to be investigated.
8. Save the new notable event. The Incident Review dashboard displays with your new notable event.