Splunk® Enterprise Security Use Splunk Enterprise Security 6.0.0

Overview of Incident Review in Splunk Enterprise Security

Generated: 11/29/2019 4:33 pm
Overview of Incident Review in Splunk Enterprise Security

The Incident Review dashboard displays notable events and their current status.

A notable event represents one or more anomalous incidents detected by a correlation search across data sources. For example, a notable event can represent:

- The repeated occurrence of an abnormal spike in network usage over a period of time
- A single occurrence of unauthorized access to a system
- A host communicating with a server on a known threat list

As an analyst, you can use the dashboard to gain insight into the severity of events occurring in your system or network. You can use the dashboard to triage new notable events, assign events to analysts for review, and examine notable event details for investigative leads.

As an administrator, you can manage and customize Incident Review and notable event settings. See Managing Incident Review in Splunk Enterprise Security for more information about administrator activities.

How Splunk Enterprise Security identifies notable events

Splunk Enterprise Security detects patterns in your data and automatically reviews events for security-relevant incidents using correlation searches. When a correlation search detects a suspicious pattern, the correlation search creates a new notable event.

The Incident Review dashboard surfaces all notable events, and categorizes them by potential severity so you can quickly triage, assign, and track issues.

Incident review workflow

You can use this example workflow to triage and work notable events on the Incident Review dashboard.

1. An administrative analyst monitors the Incident Review dashboard, sorting and performing high-level triage on newly-created notable events.
2. When a notable event warrants investigation, the administrative analyst assigns the event to a reviewing analyst to start investigating the incident.
3. The reviewing analyst updates the status of the event from **New** to **In Progress**, and begins investigating the cause of the notable event.

4. The reviewing analyst researches and collects information on the event using the fields and field actions in the notable event. The analyst records the details of their research in the **Comments** field of the notable event. As part of the research, the analyst might run adaptive response actions. If the research proves that the notable event needs more lengthy investigation, the analyst can assign the notable event to an investigation.

5. After the reviewing analyst addresses the cause of the notable event and any remediation tasks have been escalated or solved, the analyst sets the notable event status to **Resolved**.

6. The analyst assigns the notable event to a final analyst for verification.

7. The final analyst reviews and validates the changes made to resolve the issue, and sets the status to **Closed**.