

# Sending Splunk Observability events as Alert Actions from Splunk Enterprise Security

Issues identified in Splunk indexes that certain users might not have access to can still be useful for those users to be aware of. For example, Splunk Observability Cloud users might need to be aware of issues identified in Splunk Enterprise Security. An Splunk Observability Cloud Alert Action can send your developers a notification that a possible admin login brute force attack has been identified in GitHub by Splunk Enterprise Security.

This is only one example use case. Another common use case is notifying developers in Splunk Observability Cloud of DDOS attacks identified by Splunk Enterprise Security. You can use this same method to pass context from Splunk Enterprise Security to Splunk Observability Cloud.

## Solution

1. Download the [Splunk Observability Cloud Alert Action for Splunk](#) from Splunkbase.
2. From the **Apps** drop-down menu, select **Splunk Observability Cloud Alert Action for Splunk**, then click on **Configuration**.
3. Enter your Splunk Observability Cloud API token.

The screenshot shows the Splunk Configuration interface. At the top, there is a dark navigation bar with 'Configuration' and 'Search' tabs. Below this, the 'Configuration' section is active, showing 'Set up your add-on'. Under 'Add-on Settings', the 'Observability API Token' field is visible, containing a masked token (dots). A green 'Save' button is located below the token field.

4. [Create and schedule your alert](#) as normal. Here is an example of the alert setup:

Create Alert

×

Settings

Title

Code Vulnerability Found

Description

Code Vulnerability Found in Repo

Search

|from datamodel:"Code\_Vulnerabilities.Vulnerabilities" | search cve=\* AND repository\_name=\* AND is\_High\_Critical\_Vulnerabilities=1

App

DevSecOps App for Splunk (splunk\_app\_for\_devsecops) ▾

Permissions

Private

Shared in App

Alert type

Scheduled

Real-time

Run on Cron Schedule ▾

Time Range

All time ▸

Cron Expression

\*/5 \* \* \* \*

e.g. 00 18 \* \* \* (every day at 6PM). [Learn More](#)

Expires

24

hour(s) ▾

- At the bottom of your alert setup, click **Add New Response Action** then choose the **Enterprise Security to Splunk Observability** response action.

Send email

Send an email notification to specified recipients

Category: others | Task: others | Subject: others | Vendor: unknown

Enterprise Security to Splunk Observability

Send Enterprise Security data to Splunk Observability

Category: Information Conveyance | Task: update | Subject: splunk.event | Vendor: Splunk

id values specified in Fields to

ing. [Learn more](#)

+ Add New Response Action ▾

>

Notable

×

- Input the fields you would like to pass as dimensions into Splunk Observability Events.

Trigger Actions

+ Add Actions ▾

When triggered

Enterprise Security to Splunk Observability

Remove

realm \*

us0

Info field (title)

Github Admin Login Attack

Included fields

user, app, src, dest

- In Splunk Observability Cloud, open the dashboard that you'd like to overlay event data on. In the Event Overlay drop-down, choose an Event Overlay to match your event name. You can use asterisks (\*) to work as wildcards.

Overrides: Filter optional

Time -3h

Chart Resolution

Event Overlay

\*Github\*Admin\*

Save

Reset

\*Github\*Admin\*

Show Events

- In your chart options, enable **Show events as lines** and **Show data markers** for overlaying events on that chart.

Plot Editor
Chart Options
Axes
Data Table
Events

Title
Transactions per second by host and datacenter2

Visualization Options

Visualization Type

Default Time ?
-1m

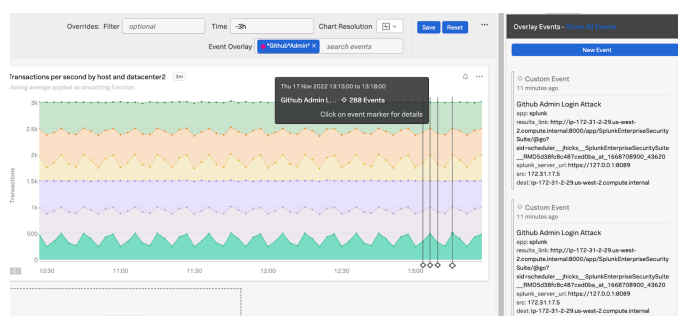
Color By ?
Dimension

☐ Include zero on Y-Axis ?

☒ Show events as lines ?

☒ Show data markers ?

Events will now be overlaid on your chart.



## Next steps

These resources might help you understand and implement this guidance:

- Splunk Docs: [Add information to a dashboard](#)
- Splunk Docs: [Create and manage organization access tokens using Splunk Observability Cloud](#)

Still need help with this use case? Most customers have [OnDemand Services](#) per their [license support plan](#). Engage the ODS team at [OnDemand-Inquires@splunk.com](mailto:OnDemand-Inquires@splunk.com) if you require assistance.