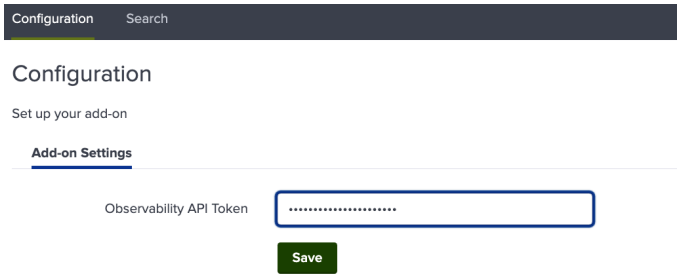
Sending Splunk Observability events as Alert Actions from Splunk Enterprise Security

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.

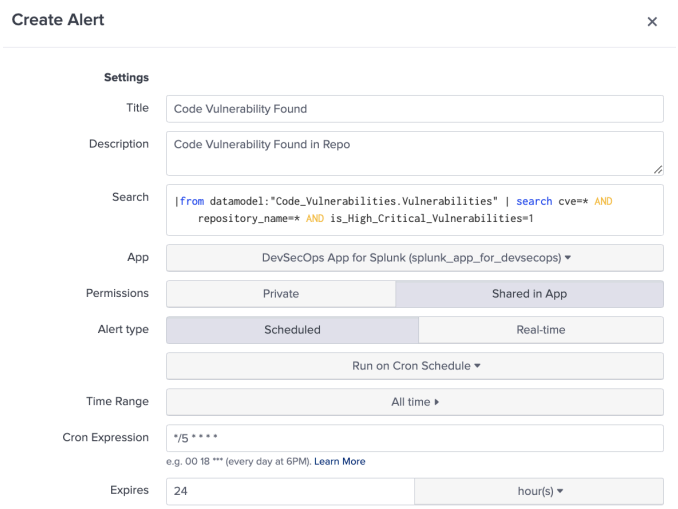
This is only one example use case. Another common use case is notifying developers in Splunk Observability Cloud of DDOS attacks identified by Splunk Enterprise Security. You can use this same method to pass context from Splunk Enterprise Security to Splunk Observability Cloud.

Solution

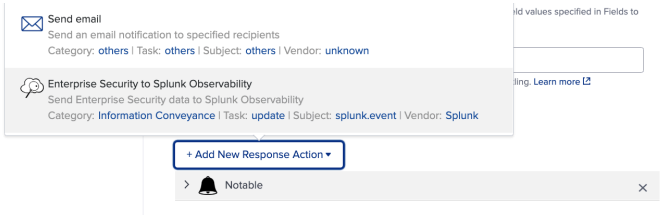
1. Download the Splunk Observability Cloud Alert Action for Splunk from Splunkbase.
2. From the **Apps** drop-down menu, select **Splunk Observability Cloud Alert Action for Splunk,** then click on **Configuration**.
3. Enter your Splunk Observability Cloud API token.



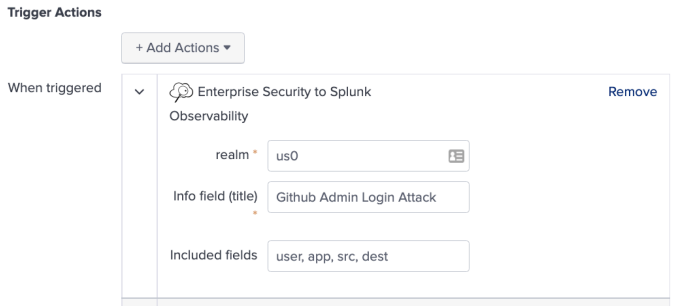
4. Create and schedule your alert as normal. Here is an example of the alert setup:



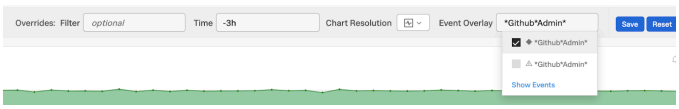
5. At the bottom of your alert setup, click **Add New Response Action** then choose the **Enterprise Security to Splunk Observability** response action.



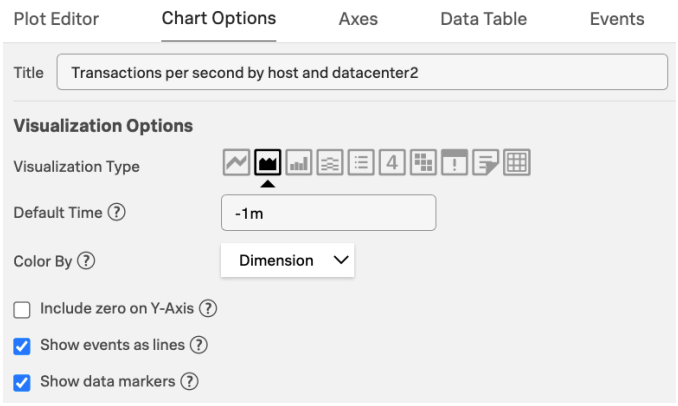
6. Input the fields you would like to pass as dimensions into Splunk Observability Events.



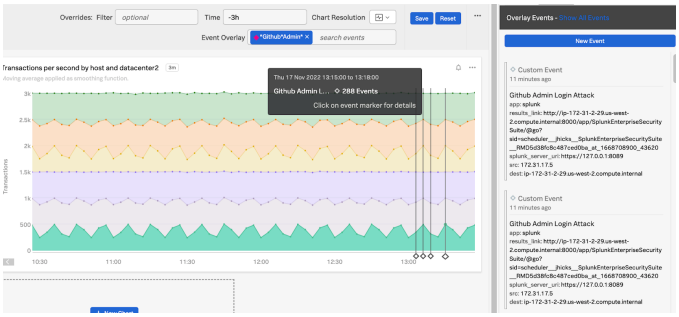
7. In Splunk Observability Cloud, open the dashboard that you'd like to overlay event data on. In the Event Overlay drop-down, choose an Event Overlay to match your event name. You can use asterisks (*) to work as wildcards.



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



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 if you require assistance.