Number of active Zoom meetings

You might need to know how many active Zoom meetings there are on your network when doing the following:

- Securing a work-from-home organization

Prerequisites

To succeed in implementing this use case, you need the following dependencies, resources, and information.

- People: Security analyst
- Technologies: Splunk Enterprise or Splunk Cloud Platform
- Data: Splunk Connect for Zoom

Example

Your workforce is fully remote. To ensure network security, you want to report on how many active Zoom meetings there are on your network at certain times of the day.

To optimize the search shown below, you should specify a time range.

1. Run the following search:

   search (index=zoom sourcetype="zoom:webhook" (event="meeting.ended" OR event="meeting.started" OR event="webinar.ended" OR event="webinar.started"))
   | stats latest(event) AS event latest(_time) AS _time BY payload.object.uuid
   | where event="meeting.started" OR event="webinar.started"
   | timechart span=1h dc(payload.object.uuid) AS active_meeting
   | sort - active_meeting
   | head 1

Search explanation

The table provides an explanation of what each part of this search achieves. You can adjust this query based on the specifics of your environment.

<table>
<thead>
<tr>
<th>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>search (index=zoom sourcetype=&quot;zoom:webhook&quot; (event=&quot;meeting.ended&quot; OR event=&quot;meeting.started&quot; OR event=&quot;webinar.ended&quot; OR event=&quot;webinar.started&quot;))</td>
<td>Search the Zoom sourcetype for events related to</td>
</tr>
</tbody>
</table>
### Splunk Search

```
OR event="webinar.ended" OR event="webinar.started")
```

### Explanation

starting and stopping Zoom meetings and webinars.

If you use a different telecommunications provider integrated with Splunk, such as Cisco WebEx Meetings Add-on for Splunk, you may need to make adjustments to the fields and parameters.

```
| stats latest(event) AS event latest(_time) AS _time BY payload.object.uuid
```

### Explanation

Calculate the time that each event occurred and sort the events by the payload object ID.

```
| where event="meeting.started" OR event="webinar.started"
```

### Explanation

Filter the results to only started meetings or webinars.

```
| timechart span=1h dc(payload.object.uuid) AS active_meeting
```

### Explanation

Create a chart that shows the distinct count of events for each payload object ID, bucketed into one hour increments.

```
| sort - active_meeting
```

### Explanation

Sort the results with the hour with the largest number of meetings first.

```
|head 1
```

### Explanation

Return only the top result.

---

**Result**

This search returns a simple count of active Zoom sessions during the time you specify. It also highlights the busiest hour in your organization. Correlate this information with the results of other searches to determine what is normal or anomalous activity on your network.