Number of all Zoom meetings created over time

You might need to know how many Zoom meetings were run in your organization 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 Zoom meetings were hosted on your network during certain time periods each 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") (TERM(meeting.ended) OR TERM(meeting.started)))
   | eval endtime = strptime('payload.object.end_time',"%FT%TZ"), starttime = strptime('payload.object.start_time',"%FT%TZ"), duration = round((endtime - starttime)/60,2)
   | timechart span=1h dc(payload.object.uuid) AS "Number of Meetings" avg(duration) AS "Average Meeting Duration (min)"

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;) (TERM(meeting.ended) OR TERM(meeting.started)))</td>
<td>Search the Zoom sourcetype for events related to</td>
</tr>
</tbody>
</table>
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.

| eval endtime = strptime('payload.object.end_time',"%FT%TZ"), starttime = strptime('payload.object.start_time',"%FT%TZ"), duration = round((endtime - starttime)/60,2)
| Parse the start and end times of the Zoom meetings into UNIX timestamps. Then, calculate the duration of each meeting, rounded to 2 decimals.

| timechart span=1h dc(payload.object.uuid) AS "Number of Meetings" avg(duration) AS "Average Meeting Duration (min)"
| Create a chart that shows the distinct count of meetings for each payload object ID and the average duration, bucketed into one hour increments.

**Result**

This search returns a table and chart of Zoom meetings held each day over the specified time frame, along with their duration. Correlate this information with the results of other searches to determine what is normal or anomalous activity on your network.