Authentication logs for an endpoint

Part of your role as a security analyst at a large organization is to monitor your network for users who access systems they don't need for their jobs. You need to set up a search to accomplish this task.

Data required

Windows event logs

Procedure

1. To complete this process, you should ensure you are ingesting normalized data, populating the Authentication data model in the Common Information Model (CIM). For information on installing and using the CIM, see the Common Information Model documentation.

2. Run the following search. You can optimize it by specifying an index and adjusting the time range.

   ```bash
   |tstats count FROM datamodel=Authentication WHERE Authentication.dest=<dest ip> BY _time, Authentication.dest, Authentication.user, Authentication.app, Authentication.action
   rename "Authentication.*" as "*"
   ```

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></td>
<td>tstats count FROM datamodel=Authentication WHERE Authentication.dest=&lt;dest ip&gt; BY _time, Authentication.dest, Authentication.user, Authentication.app, Authentication.action</td>
</tr>
<tr>
<td>rename &quot;Authentication.&quot; as &quot;*&quot;</td>
<td>Rename the data model object for better readability.</td>
</tr>
</tbody>
</table>

Next steps

The results show the time, user, application, and action related to authentication to a specific destination. You can investigate users who you believe should not have authenticated to that particular endpoint.
Finally, you might be interested in other processes associated with the following use cases:

- Detecting techniques in the Orangeworm attack group
- Monitoring Windows account access
- Monitoring for signs of Windows privilege escalation attacks