Secure facilities access auditing

You might need to audit and report on security facilities access when doing the following:

- Monitoring badges for facilities access

Prerequisites

In order to execute this procedure in your environment, the following data, services, or apps are required:

- Splunk Enterprise or Splunk Cloud Platform
- Physical card reader data for call detail records
- A CSV or KV lookup file that maps badge reader IDs to their location
- A CSV or KV lookup file that maps user badge IDs to user information

Example

Auditing of physical access is often a requirement for regulatory bodies and industrial certifications. You need to be able to associate ingress and egress traffic for designated rooms and zones to specific badges in near real-time.

To optimize the search shown below, you should specify a time range. You may also need to adjust field names to match what is available in your lookup files.

1. Ensure your lookup file is uploaded to your Splunk deployment.
2. Run the following search:

```
| source=<physical card reader logs>
| lookup <badge reader ID to location mapping> readerID AS badgereaderId OUTPUTNEW description
| lookup <badge to user info mapping> cardId AS badgeId
| search description="LV-DC-2-DC-003-*"
| stats count list(description) AS Room list(status) AS Status list(badgeId) AS BadgeID list(employeeId) AS userId BY _time
| eval Personnel=if(match(userId,"-"),"Customer Card","Datacenter Staff")
| eval Direction=case(match(Room,"-in"),"Ingress",match(Room,"-out"),"Egress")
| eval Room=case(match(Room,"LV-DC-2-DC-003"),"Secure Room - 3")
| fields _time Room Personnel Direction
| rename _time AS "Time"
| convert ctime(Time)
```

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
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>sourcetype=&lt;physical card reader logs&gt;</td>
</tr>
<tr>
<td></td>
<td>lookup &lt;badge reader ID to location mapping&gt; readerID AS badgereaderId OUTPUTNEW description active</td>
</tr>
<tr>
<td></td>
<td>lookup &lt;badge to user info mapping&gt; cardId AS badgeId</td>
</tr>
<tr>
<td></td>
<td>search description=&quot;LV-DC-2-DC-003-*.&quot;</td>
</tr>
<tr>
<td></td>
<td>stats count list(description) AS Room list(status) AS Status list(badgeId) AS BadgeID list(employeeId) AS userId BY _time</td>
</tr>
<tr>
<td></td>
<td>eval Personnel=if(match(userId,&quot;-&quot;),&quot;Customer Card&quot;,&quot;Datacenter Staff&quot;)</td>
</tr>
<tr>
<td></td>
<td>eval Direction=case(match(Room,&quot;-in&quot;),&quot;Ingress&quot;,match(Room,&quot;-out&quot;),&quot;Egress&quot;)</td>
</tr>
<tr>
<td></td>
<td>eval Room=case(match(Room,&quot;LV-DC-2-DC-003-&quot;),&quot;Secure Room - 3&quot;)</td>
</tr>
<tr>
<td></td>
<td>fields _time Room Personnel Direction</td>
</tr>
<tr>
<td></td>
<td>rename _time AS &quot;Time&quot;</td>
</tr>
<tr>
<td></td>
<td>convert ctime(Time)</td>
</tr>
</tbody>
</table>
Result

Reporting from this may potentially be used for security, compliance, or customer reporting requirements.