Kubernetes role-based access control authorizations

You might want information about Kubernetes RBAC authorizations when doing the following:

- Monitoring Kubernetes sensitive role activities

Prerequisites

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

- Splunk Enterprise or Splunk Cloud Platform
- Kubernetes
- One of the following:
  - Amazon: Splunk Add-on for Amazon Web Services, Splunk App for AWS, and AWS CloudWatch data
  - Microsoft: Splunk Add-on for Microsoft Cloud Services and Azure storage data
  - Google: Splunk Add-on for Google Cloud Platform and Pub/Sub data

Example

Not all RBAC authorizations are malicious, but they can uncover malicious activity, especially if sensitive roles have been granted. You want to review RBAC authorizations on your network to determine if they represent a threat.

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

AWS

1. Ensure that your deployment is ingesting CloudWatch logs.
2. Run the following search:

```bash
sourcetype="aws:cloudwatchlogs:eks" annotations.authorization.k8s.io/reason=* | table sourceIPs{} user.username userAgent annotations.authorization.k8s.io/reason | stats count BY user.username annotations.authorization.k8s.io/reason | rare user.username annotations.authorization.k8s.io/reason
```

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.
### Splunk Search

| sourcetype="aws:cloudwatchlogs:eks" | Search only AWS EKS Kubernetes data. |
| annotations.authorization.k8s.io/reason=* | Search for authorizations with any reason. |

| table sourceIPs{} user.username userAgent annotations.authorization.k8s.io/reason | Display the results in a table with columns in the order shown. |
| stats count BY user.username annotations.authorization.k8s.io/reason | Count the number of authorizations by user and reason. |
| rare user.username annotations.authorization.k8s.io/reason | Return the least common usernames authorized and the reasons. |

---

### Azure

1. Ensure that you have configured Kube-Audit data diagnostics.
2. Run the following search:

   sourcetype:mscs:storage:blob:json category=kube-audit
   | spath input=properties.log
   | search annotations.authorization.k8s.io/reason=*
   | table sourceIPs{} user.username userAgent annotations.authorization.k8s.io/reason
   | stats count BY user.username annotations.authorization.k8s.io/reason
   | rare user.username annotations.authorization.k8s.io/reason

**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.

---

### Splunk Search

| category=kube-audit | Search the data source kube-audit from the diagnostic logs in Azure Cloud services. |
### Splunk Search

<table>
<thead>
<tr>
<th>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>`</td>
<td>spath input=properties.log</td>
</tr>
<tr>
<td>`</td>
<td>search annotations.authorization.k8s.io/reason=*</td>
</tr>
<tr>
<td>`</td>
<td>table sourceIPs{} user.username userAgent annotations.authorization.k8s.io/reason</td>
</tr>
<tr>
<td>`</td>
<td>stats count BY user.username annotations.authorization.k8s.io/reason</td>
</tr>
<tr>
<td>`</td>
<td>rare user.username annotations.authorization.k8s.io/reason</td>
</tr>
</tbody>
</table>

### GCP

1. Ensure that your deployment is ingesting Pub/Sub messaging logs.
2. Run the following search:

   ```splunk
   sourcetype="google:gcp:pubsub:message" data.labels.authorization.k8s.io/reason=ClusterRoleBinding OR Clusterrole
   | table src_ip src_user data.labels.authorization.k8s.io/decision data.labels.authorization.k8s.io/reason
   | rare src_user data.labels.authorization.k8s.io/reason
   ```

### 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><code>sourcetype=&quot;google:gcp:pubsub:message&quot;</code></td>
<td>Search only GCP Pub/Sub messages.</td>
</tr>
<tr>
<td><code>data.labels.authorization.k8s.io/reason=ClusterRoleBinding OR Clusterrole</code></td>
<td>Search for high-privilege, role-based authorizations such as cluster role binding and cluster role.</td>
</tr>
</tbody>
</table>

---

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.
| table src_ip src_user data.labels.authorization.k8s.io/decision data.labels.authorization.k8s.io/reason |
| rare src_user data.labels.authorization.k8s.io/reason |

Display the results in a table with columns in the order shown.

Show the least common occurrences of these authorizations.

Result

The reasons provided in this search may provide context on unusual role based authorizations by specific users. Contextual items include:

- Source IP addresses: Are they part of security groups or do they match IP address reputation?
- Source user and geolocation of an IP address: When correlating this information with access to high privilege roles, you might identify suspicious or malicious activity. For example, you might find an IP address from an unusual region associated with a user not expected from that region and access to high privilege roles within a cluster.
- Restricted clusters: Unless the cluster contains an application exposed to the internet, access from specific IP addresses and specific users must be monitored, especially if the interactions are with high privilege roles within the cluster.

Cross account activity investigation may be needed to provide more context. For example, are these unusual IP addresses and source users accessing other clusters or resources from the named cluster that produces these alerts? Are new resources (such as pods, volumes, or applications) being created. Note also that this search can be modified by adding top to see both extremes of RBAC by accounts occurrences.

For additional information about this search, such as its applicability to common frameworks and standards, see this project on GitHub for AWS, Azure, or GCP.

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.