Kubernetes sensitive roles

You might want information about Kubernetes ClusterRoles and ClusterRoleBindings, which have elevated namespace and cluster permissions, 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

Sensitive role resource access is necessary for cluster operation, however, you want to make sure roles with permission to sensitive objects aren't using their privileges for malicious ends. You want to investigate sensitive roles 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" objectRef.resource=clusterroles OR clusterrolebindings sourceIPs{}!=::1 sourceIPs{}!=<valid IP address> | table sourceIPs{} user.username user.groups{} objectRef.namespace requestURI annotations.authorization.k8s.io/reason | dedup user.username user.groups{}
```

Search explanation

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.
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>sourcetype=&quot;aws:cloudwatchlogs:eks&quot;</td>
<td>Search only AWS EKS Kubernetes data.</td>
</tr>
<tr>
<td>objectRef.resource=clusterroles OR clusterrolebindings</td>
<td>Search for events from the sensitive roles, clusterrole or clusterrolebindings.</td>
</tr>
<tr>
<td>sourceIPs{}!=::1 sourceIPs{}!=&lt;valid IP address&gt;</td>
<td>Exclude a legitimate IP address or range of addresses from the search.</td>
</tr>
<tr>
<td></td>
<td>Display the results in a table with columns in the order shown.</td>
</tr>
<tr>
<td>dedup user.username user.groups{}</td>
<td>Remove duplicate results from the same IPs and users.</td>
</tr>
</tbody>
</table>

---

**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 objectRef.resource=clusterroles OR clusterrolebindings
| table sourceIPs{} user.username user.groups{} objectRef.namespace requestURI annotations.authorization.k8s.io/reason
| dedup user.username user.groups{}
```

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>
</table>
Splunk Search

category=kube-audit

| spath input=properties.log
| search objectRef.resource=clusterroles OR clusterrolebindings
| table sourceIPs{} user.username user.groups{} objectRef.namespace requestURI annotations.authorization.k8s.io/reason
| dedup user.username user.groups{}

Explanation

Search the data source kube-audit from the diagnostic logs in Azure Cloud services.

Extract fields from the properties Kube-Audit log.

Search for events from the sensitive roles, clusterrole or clusterrolebindings.

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

Remove duplicate results from the same IPs and users.

GCP

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

   sourcetype="google:gcp:pubsub:message" data.labels.authorization.k8s.io/reason=ClusterRoleBinding OR Clusterrole dest=apis/rbac.authorization.k8s.io/v1 src_ip!::1
   | table src_ip src_user http_user_agent data.labels.authorization.k8s.io/decision data.labels.authorization.k8s.io/reason
   | dedup src_ip src_user

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="google:gcp:pubsub:message"

data.labels.authorization.k8s.io/reason=ClusterRoleBinding OR Clusterrole

Explanation

Search only GCP Pub/Sub messages.

Search for events from the sensitive roles, clusterrole or clusterrolebindings.

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.
Splunk Search

dest=apis/rbac.authorization.k8s.io/v1

src_ip!::1

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

| dedup src_ip src_user

Explanation

Search events with this destination path.

Exclude a legitimate range of addresses from the search.

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

Remove duplicate results from the same IPs and users.

Result

If any of the following appear in your results, you should investigate further:

• Unknown IP addresses
• Unauthenticated or unknown usergroups that request access to sensitive roles
• Unusual geographical location, access times, or reasons

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**.