Most active Kubernetes service accounts

You might want information about activity levels of Kubernetes service accounts 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

Service accounts are prime targets for attackers as they may present the opportunity to obtain credentials and move across all the resources they access. You want to investigate the most active Kubernetes service accounts for each pod to determine if their activities 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:

   sourceType="aws:cloudwatchlogs:eks" user.groups{}=system:serviceaccounts objectRef.resource=pods | table sourceIPs{} user.username userAgent verb annotations.authorization.k8s.io/decision | top sourceIPs{} user.username verb annotations.authorization.k8s.io/decision

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>sourcetype=&quot;aws:cloudwatchlogs:eks&quot;</td>
<td>Search only AWS EKS Kubernetes data.</td>
</tr>
<tr>
<td>user.groups{}=system:serviceaccounts</td>
<td>Search the service accounts user group.</td>
</tr>
<tr>
<td>objectRef.resource=pods</td>
<td>Search your Kubernetes pods data.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Display the results in a table with columns in the order shown.</td>
</tr>
<tr>
<td></td>
<td>Show the 10 most active (by count and percentage) IP addresses, usernames, and request verbs (for example, list) with the respective decision (for example, deny or forbid).</td>
</tr>
</tbody>
</table>

### Azure

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

```splunk
sourcetype=mscs:storage:blob:json category=kube-audit | spath input=properties.log | search user.groups{}=system:serviceaccounts* OR user.username=system.anonymous OR annotations.authorization.k8s.io/decision=allow | table sourceIPs{} user.username userAgent verb responseStatus.reason responseStatus.status properties.pod objectRef.namespace | top sourceIPs{} user.username verb responseStatus.status properties.pod objectRef.namespace
```

**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><strong>Splunk Search</strong></td>
<td><strong>Explanation</strong></td>
</tr>
<tr>
<td>------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>category=kube-audit</td>
<td>Search the data source kube-audit from the diagnostic logs in Azure Cloud services.</td>
</tr>
<tr>
<td>spath input=properties.log</td>
<td>Extract fields from the properties Kube-Audit log.</td>
</tr>
<tr>
<td></td>
<td>Search the service account user group or anonymous access or any requests with allow decisions.</td>
</tr>
<tr>
<td></td>
<td>Display the results in a table with columns in the order shown.</td>
</tr>
<tr>
<td></td>
<td>Show the 10 most active (by count and percentage) source IP addresses, usernames, request verbs (for example, list), response statuses, pods and namespaces.</td>
</tr>
</tbody>
</table>

**GCP**

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

   sourcetype="google:gcp:pubsub:message" data.protoPayload.request.spec.group{}=system:serviceaccounts | table src_ip src_user http_user_agent data.protoPayload.request.spec.nonResourceAttributes.verb data.labels.authorization.k8s.io/decision data.protoPayload.response.spec.resourceAttributes.resource | top src_ip src_user http_user_agent data.labels.authorization.k8s.io/decision data.protoPayload.response.spec.resourceAttributes.resource

**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

```splunk
sourcetype="google:gcp:pubsub:message"
```

**Explanation**

Search only GCP Pub/Sub messages.

```splunk
data.protoPayload.request.spec.group{}=system:service accounts
```

**Explanation**

Search the service account user group.

```splunk
| table src_ip src_user http_user_agent
data.protoPayload.request.spec.nonResourceAttributes.verb
data.labels.authorization.k8s.io/decision
data.protoPayload.response.spec.resourceAttributes.resource
```

**Explanation**

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

```splunk
| top src_ip src_user http_user_agent
data.labels.authorization.k8s.io/decision
data.protoPayload.response.spec.resourceAttributes.resource
```

**Explanation**

Show the 10 most active (by count and percentage) source IP addresses, users, user agents, and the respective decisions on targeted resources.

---

### Result

Not all service accounts interactions are malicious. Analysts must consider IP address, verb, and decision context when trying to detect maliciousness. Service accounts are usually created for specific tasks, so a number of unusual failures, deny statuses, or forbidden statuses may indicate suspicious activity. IP addresses must be restricted by security groups or allow/deny policies, unless a cluster API must be exposed.

For additional information about this search, such as its applicability to common frameworks and standards, see this project on GitHub for [AWS](https://github.com/aws), [Azure](https://github.com/Azure), or [GCP](https://github.com/google).