Azure Kubernetes pod scan fingerprinting

Kubernetes pods are a group of one or more containers with shared storage and a specification for how to run the containers. A pod's contents are always co-located and co-scheduled. You might want to look for fingerprinting scans against Kubernetes pods when doing the following:

- Detecting Kubernetes scanning activity

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
- Azure Storage data
- Splunk Add-on for Microsoft Cloud Services

Example

One of your concerns with using Kubernetes is fingerprinting. You want to know if your pods are being targeted, and, if so, to get details about the files or directories being probed.

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

1. Ensure that you have configured Kube-Audit data diagnostics in the Splunk Add-on for Microsoft Cloud Services.
2. Run the following search:

```
sourcetype:mscs:storage:blob:json category=kube-audit
| spath input=properties.log
| search responseStatus.code=401
| table sourceIPs() userAgent verb requestURI responseStatus.reason properties.pod
```

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>category=kube-audit</td>
<td>Search the data source kube-audit from the diagnostic logs in Azure Cloud services.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Pull information from this specific Kubernetes audit log.</td>
</tr>
<tr>
<td></td>
<td>Search for HTTP Status 401, an unauthorized request.</td>
</tr>
<tr>
<td></td>
<td>Display the results in a table with columns in the order shown.</td>
</tr>
</tbody>
</table>

**Result**

The results provide an IP address, user agent, verb, request URI, and response status. Not all unauthenticated requests are malicious, but these strings can provide clues of the type of tool being used for scanning. Watch for IP addresses flagged as malicious by popular IP reputation lists, such as [Team Cymru](https://www.cymru.com), and analyze the HTTP verb in relation to the user agent, suspicious IP address, and the target URI to understand the intentions of detected scans.

For additional information about this search, such as its applicability to common frameworks and standards, see this [project on GitHub](https://github.com/details).