Threat signatures used to investigate a cyberattack

Known malware can have existing intrusion detection and intrusion prevention signatures that fire in response to a threat. Knowing what signatures fired can help you understand when the threat was seen, where in the network it was seen, what technology identified the signature, and the nature of the threat. Signatures can speed up investigations when doing the following:

- **Investigating a ransomware attack**

Prerequisites

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

- Splunk Enterprise or Splunk Cloud Platform
- System log data

Example

You have identified a malware attack on your network and need to gather as much information about the threat as quickly as possible to start an investigation. You decide to look at threat signatures first.

To optimize the search shown below, you should specify an index and a time range. In addition, this sample search uses Suricata data. You can replace this source with any other system log data used in your organization.

1. Run the following search:

```
|sourcetype=suricata alert.signature=*<name of threat>*
|stats count BY alert.signature alert.signature.id
|eval time=strftime(time,"%c")
|sort count
```

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.

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>
<thead>
<tr>
<th>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourcetype=suricata</td>
<td>Search only Suricata log data.</td>
</tr>
<tr>
<td>alert.signature=<em>&lt;name of threat&gt;</em></td>
<td>Search for events that include the name of the known threat.</td>
</tr>
<tr>
<td></td>
<td>stats count BY alert.signature alert.signature.id</td>
</tr>
<tr>
<td></td>
<td>eval time=strftime(time,&quot;%c&quot;)</td>
</tr>
<tr>
<td></td>
<td>sort count</td>
</tr>
</tbody>
</table>

**Result**

The results show all combinations of alert signatures and alert signature IDs, along with the times they fired and the number of times they fired. You can compare the times a signature fired to times unexpected processes fired to help establish a cause-and-effect relationship.