Microsoft recommended application log events

A solid event log monitoring system is a crucial part of any secure Windows environment or Active Directory design. Many computer security compromises could be discovered early if the victims enacted appropriate event log monitoring and alerting. This search leverages application monitoring recommendations provided by Microsoft to identify whether an event should be considered of low, medium, or high criticality in detecting attacks and errors.

Data required

Windows update logs

Procedure

1. Verify that you deployed the Splunk Add-on for Microsoft Windows add-on to your search heads, indexer, and Splunk Universal Forwarders on the monitored systems. For more information, see About installing Splunk add-ons.

2. Run the following search. You can optimize it by specifying an index and adjusting the time range.

```
sourcetype=WinEventLog
  | inputlookup app_log_evt_code_desc WHERE LogName='"Application"'
  | stats values(EventCode) AS EventCode BY LogName
  | format
| fields _time,host,LogName,EventCode,signature,signature_severity
| stats max(_time) AS l_time, dc(host) AS host_count,last(host) AS last(host),count BY LogName,EventCode,signature,signature_severity
| table count,LogName,EventCode,signature,signature_severity
| append
  | inputlookup ms_ad_obj_evt_code_desc
  | eval count=0
  | table LogName,EventCode,signature,signature_severity
| stats max(count) AS Total_Events BY LogName,EventCode,signature_severity,signature
| fillnull value="0" Total_Events
| sort -Total_Events
```

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><strong>Splunk Search</strong></th>
<th><strong>Explanation</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>sourcetype=WinEventLog</td>
<td>Search only Windows event logs.</td>
</tr>
</tbody>
</table>

Get a list of recommended EventCode IDs from a lookup table and match the codes to the events. You can add IDs to the table if needed. The lookup is then leveraged in a subsearch against your Windows events across multiple dashboards, reports, and alerts. By leveraging this approach, you can easily create scheduled reports or alerts for when any of the recommended event IDs appear in your data. For example, if you want to create an alert for high severity events, such as Application Error, Application Hang, or Update Failures, you can add (WHERE severity="High") to the lookup table in the search: `| inputlookup app_log_evt_code_desc WHERE LogName="Application" AND severity="High"`. |

Include only the fields shown in the results. Return times and distinct counts that these events occurred on your hosts. Display the results in a table with columns in the order shown. Append data from any related lookup files for the same event code IDs. Provide a count for each event and sort the results first by LogName and then by other fields. Set the Total_Events field to 0 if null. This will be a rare occurrence.

---

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

| sort -Total_Events |

#### Explanation

Sort with the event with the highest count first.

### Next steps

The following table shows sample search results. It shows what events took place, ordered by count of events (Total_Events). The other columns give descriptions of the events. From the table, you can decide what to further summarize or pay attention to.

<table>
<thead>
<tr>
<th>LogName</th>
<th>EventCode</th>
<th>severity</th>
<th>Event_Type</th>
<th>signature</th>
<th>Total_Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>4624</td>
<td>informational</td>
<td>Information</td>
<td>An account was successfully logged on</td>
<td>52480</td>
</tr>
<tr>
<td>Security</td>
<td>4625</td>
<td>informational</td>
<td>Information</td>
<td>An account failed to log on</td>
<td>24504</td>
</tr>
<tr>
<td>Application</td>
<td>1001</td>
<td>informational</td>
<td>Information</td>
<td>Windows Error Reporting</td>
<td>9856</td>
</tr>
<tr>
<td>Security</td>
<td>5136</td>
<td>informational</td>
<td>Active Directory Domain Services</td>
<td>A directory service object was modified</td>
<td>8024</td>
</tr>
<tr>
<td>Application</td>
<td>1001</td>
<td>medium</td>
<td>Warning</td>
<td>Windows Error Reporting</td>
<td>1696</td>
</tr>
</tbody>
</table>

While the search provided above gives a full picture of event codes that occur in your network, you might find a targeted search for risky errors more useful. After understanding the general state of your applications, you could run the following search to identify specific computers and users who are linked to application logs that can benefit from further investigation:

```
| sourcetype=wineventlog Type=ERROR OR severity=high
|stats count BY Type severity ComputerName User
```

You can save the search and results as a dashboard, a report (saved search), or as an alert and associate an action with the event, such as opening a ticket or sending a notification to the on call help desk for rapid action.
Finally, you might be interested in other processes associated with the [Maintaining Microsoft Windows systems](#) use case.