Device with outdated anti-malware

Malware can persist if an endpoint protection solution does not update its malware signatures. Even a single host with outdated anti-malware can indicate an infection. You want to search for outdated anti-malware to keep your devices safe.

Required data

Antivirus data. This sample search uses Symantec Endpoint Protection. You can replace this source with any other antivirus data used in your organization.

Procedure

1. Identify all relevant IT assets from a data mapping exercise conducted by the Data Privacy Officer’s team. These are all IT assets that are relevant to the full audit trail of data processing activities. This includes not only data stores and repositories that house sensitive personal data (PD) and personally identifiable information (PII), but also any technologies that are involved in the processing, storage, transmission, receipt, rendering, encrypt/decrypt, relaying, and handling of such data in any capacity.
2. Ensure that those assets are configured properly to report logging activity to an appropriate central repository.
3. Use your data mapping results to build a lookup that associates systems to their system category.
4. Run the following search. You can optimize it by specifying an index and adjusting the time range.

```
sourcetype=symantec:* |stats max(eval(if(like(Event_Description, "%LiveUpdate session ran successfully") , _time, null))) AS LatestUpdate max(_time) AS LatestMessage max(eval(if(tag="error", _time, null))) AS LatestError BY Host_Name |where LatestUpdate < relative_time(LatestMessage, "-3d") OR LatestError > LatestUpdate |lookup <name of lookup you created in step 3> host |search category=* |convert ctime(LatestUpdate) ctime(LatestMessage) ctime(LatestError)
```

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=symantec:*</td>
<td>Search only Symantec Endpoint data.</td>
</tr>
</tbody>
</table>
### Splunk Search

|stats max(eval(if(like(Event_Description, "%LiveUpdate session ran successfully\%") , _time, null))) AS LatestUpdate max(_time) AS LatestMessage max(eval(if(tag="error", _time, null))) AS LatestError BY Host_Name

### Explanation

Track the time of the last update and the time of the last error. This relies on string matches of free form text in the Event_Description field. Other source types will need a similar or different method for detecting success or failure status for signature updates.

|where LatestUpdate < relative_time(LatestMessage, "-3d") OR LatestError > LatestUpdate

Filter for the events where the time of the last update was more than three days ago or where the last error was more recent than the last update.

|lookup <name of lookup you created in step 3> host as Host_Name OUTPUT category

Look up the host in the categorization lookup you created. When the host in the lookup matches dest in the event, output the category value from the lookup and add it to the event.

|search category=* 

Filter for events that have a value in the category field. These are in-scope for GDPR compliance.

|convert ctime(LatestUpdate) ctime(LatestMessage) ctime(LatestError)

Convert this time into a readable string

### Next steps

Identify the in-scope systems with outdated anti-malware or lacking anti-malware protection, pinpoint the root issue for updates not occurring, and remediate those hosts by configuring them or the environment appropriately, depending on what the root issue turns out to be. If you don’t see an obvious reason (e.g., specific and logical error), then it may be worth investigating that host to see if there are any other suspicious events that have occurred to rule out an infection.

Additionally, you should monitor the mapped IT assets changes in logging status, adjust for known outages, and prioritize incident response for any failures to report by hosts that are not scheduled for downtime.

**GDPR Relevance:** When environments that are involved in processing personal data include systems with outdated anti-malware protection (or lacking protection altogether), those systems are at high risk, and therefore out of compliance with the GDPR regulation to maintain and prove privacy requirements are being met per Article 32, Article 58, and Article 82. If a host is tagged under the GDPR category, then immediate remediation is required to address that non-compliant condition.

---

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.
Finally, you might be interested in other processes associated with the [Complying with General Data Protection Regulation](Complying with General Data Protection Regulation) use case.