NIST SP 800-53 system and information integrity

You need to monitor cybersecurity data and services provided by point solutions for compliance with NIST SP 800-53 rev5.

Required data

- Data normalized to the following Common Information Models:
  - Authentication
  - Intrusion Detection
  - Malware
  - Web

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

Malicious code protection

These searches help you implement malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code.

Hosts with an infection

To count how many hosts on your network have been identified as having a malware infection, run the following search.

```
| tstats count FROM datamodel=Malware BY Malware_Attacks.dest
| stats dc(Malware_Attacks.dest) AS total
```

Hosts with multiple infections

To get a list of hosts that have more than one malware infection, run the following search. You can change the `sum_signatures > 1` argument to a value greater than one if needed.

```
| tstats dc(Malware_Attacks.signature) FROM datamodel=Malware BY Malware_Attacks.dest
| rename Malware_Attacks.dest AS dest dc(Malware_Attacks.signature) AS sum_signatures
| eval multi_infections = if(sum_signatures > 1, 1, 0)
| stats sum(multi_infections)
| rename sum(multi_infections) AS Endpoints
```
Malware detection by time

To see how many malware attacks hit your system over time, run the following search. You can run the same search for `Malware_Attacks.action` instead of `Malware_Attacks.signature` if needed.

```
| tstats count FROM datamodel=Malware BY _time Malware_Attacks.signature span=1s
| timechart sum(count) BY Malware_Attacks.signature useother=0 usenull=0
| fillnull value=0
```

Web proxy categorization flow

To see data about web proxy categorizations on your network, run the following search.

```
| rename Web.user AS user Web.category AS category Web.url AS url
| stats count BY user, category, url
| appendpipe [stats count by user, category | rename user AS source, category AS target]
| appendpipe [stats count BY category, url | rename category AS source, url AS target]
| search source=* 
| fields source target count
```

Attack categories observed

To get a count of the attack categories observed on your systems, run the following search.

```
| tstats count FROM datamodel=Intrusion_Detection.IDS_Attacks WHERE IDS_Attacks.ids_type=network BY IDS_Attacks.category
| rename IDS_Attacks.category AS category
| sort -count
```

System monitoring

These searches help you monitor your systems to detect attacks and indicators of potential attacks.

Endpoint malware protection actions

To see how many malware protective actions your system took over time, run the following search. You can change the `span` to a value other than one second.

```
| tstats count FROM datamodel=Malware BY _time Malware_Attacks.action span=1s
| timechart sum(count) BY Malware_Attacks.action useother=0 usenull=0
| fillnull value=0
```
Endpoint malware protection detections

To see how many malware attacks hit your system over time, run the following search. You can change the `span` to a value other than one second.

```
| tstats count FROM datamodel=Malware BY _time Malware_Attacks.signature span=1s
| timechart sum(count) BY Malware_Attacks.signature useother=0 usenull=0
| fillnull value=0
```

Attack categories observed

To get a count of the attack categories observed on your systems, run the following search.

```
| tstats count FROM datamodel=Intrusion_Detection.IDS_Attacks WHERE IDS_Attacks.ids_type=network BY IDS_Attacks.category
| rename IDS_Attacks.category AS category
| sort -count
```

Login failures

To get a count of failed logins to your systems, run the following search. You can change the `span` to a value other than one day.

```
| tstats count FROM datamodel=Authentication WHERE nodename=Authentication.Failed_Authentication BY _time, Authentication.src, Authentication.dest, Authentication.user  span=1d
```

Next steps

After running these access controls and taking appropriate action, you may want to look into other NIST SP 800-53 rev5 controls:

- Access control
- Audit and accountability
- Configuration management
- Identification and authentication
- Incident response
- Risk assessment

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.