NIST SP 800-53 risk assessment

You want to scan for vulnerabilities in your system and hosted applications on a recurring basis to be able to identify and report on new vulnerabilities potentially affecting the systems. This assessment of your information technology risk posture will help with compliance to NIST SP 800-53 rev5.

Required data

- Data normalized to the following Common Information Model:
  - Vulnerabilities

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

Count of vulnerable systems with vulnerabilities across the enterprise

To see how many systems in your organization have been classified with a critical or high vulnerability, run the following search.

| tstats count FROM datamodel=Vulnerabilities BY Vulnerabilities.dest, Vulnerabilities.cve, Vulnerabilities.severity, Vulnerabilities.signature, Vulnerabilities.cvss | search (Vulnerabilities.severity="critical" OR Vulnerabilities.severity="high") | stats dc(Vulnerabilities.dest) |

Percentage of systems with vulnerabilities across the enterprise

To see what percentage of systems in your organization have been classified with a critical or high vulnerability, run the following search.

| tstats dc(Vulnerabilities.dest) AS all_systems_scanned FROM datamodel=Vulnerabilities | appendcols [] tstats dc(Vulnerabilities.dest) AS vulnerable FROM datamodel=Vulnerabilities WHERE (Vulnerabilities.severity="critical" OR Vulnerabilities.severity="high") | eval percent_vuln = (vulnerable/all_systems_scanned)*100 | top percent_vuln |

Count of vulnerabilities by severity

To calculate a count of systems that have each each vulnerability rating, run the following search.

| tstats count FROM datamodel=Vulnerabilities BY Vulnerabilities.dest, Vulnerabilities.cve, Vulnerabilities.severity, Vulnerabilities.signature, Vulnerabilities.cvss |

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.
Vulnerability trend by severity

To see how many of your systems have each vulnerability rating over a certain time period, run the following search. You can also change the `time_span` to a value other than two minutes.

```
| tstats count FROM datamodel=Vulnerabilities WHERE (Vulnerabilities.severity="critical" OR Vulnerabilities.severity="high") BY _time span=1s, Vulnerabilities.dest Vulnerabilities.severity Vulnerabilities.cve
| rename Vulnerabilities.severity AS Severity
| timechart sum(count) AS count BY Severity
| fillnull value=0
```

Top 10 systems by vulnerability count

To see your top ten systems with the most critical and high vulnerability ratings, run the following search.

```
| tstats count FROM datamodel=Vulnerabilities BY Vulnerabilities.dest, Vulnerabilities.cve, Vulnerabilities.severity, Vulnerabilities.signature, Vulnerabilities.cvss
| search (Vulnerabilities.severity="critical" OR Vulnerabilities.severity="high")
| dedup Vulnerabilities.dest Vulnerabilities.severity Vulnerabilities.cve
| stats count BY Vulnerabilities.severity Vulnerabilities.dest
| chart limit=10 sum(count) OVER Vulnerabilities.dest BY Vulnerabilities.severity
| addtotals
| sort -Total
| head 10
| fields - Total
```

Recent vulnerabilities identified

To see a table of the most identified vulnerability signatures in your systems, run the following search.

```
| tstats count FROM datamodel=Vulnerabilities WHERE (Vulnerabilities.severity="critical" OR Vulnerabilities.severity="high") AND (Vulnerabilities.cve="**") BY Vulnerabilities.dest Vulnerabilities.cve Vulnerabilities.signature Vulnerabilities.cvss
| rename Vulnerabilities.cve AS CVE, Vulnerabilities.signature AS Signature, Vulnerabilities.cvss AS CVSS, Vulnerabilities.dest AS Host
| table CVSS, Host, Signature, CVE
| sort -CVSS
```
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
- System and information integrity