Tenable.sc

Tenable.sc is a vulnerability management solution that provides visibility into the security posture of your distributed and complex IT infrastructure. It consolidates and evaluates vulnerability data from across your entire IT infrastructure, illustrates vulnerability trends over time, and assesses risk with actionable context for effective remediation prioritization. In the Common Information Model, Tenable.sc data can be mapped to [Vulnerabilities](#) data model.

### Configuration

Guidance for onboarding data can be found in the Splunk Documentation, [Getting Data In](#) (Splunk Enterprise) or [Getting Data In](#) (Splunk Cloud). In addition, Tenable maintains documentation for its Splunk integrations [here](#). Refer to the documentation, and note the following:

- **Source types**
  - tenable.sc.vuln
  - tenable.sc.assets
  - tenable.sc.plugin
- **Input type:** Various for Tenable.sc Vulnerability and Tenable.sc Mobile
- **Add-on or app**
  - Tenable Add-On for Splunk
  - Tenable App for Splunk
  - Tenable.sc

### Application

When your Splunk deployment is ingesting Tenable.sc data, you can use the data to achieve the following:

- Meeting government compliance standards
- Detecting Supernova web shell malware