Container data

Container logs are an efficient way to acquire logs generated by applications running inside a container. By utilizing logging drivers, output that is usually logged is redirected to another target. Since logging drivers start and stop when containers start and stop, this is the most effective way of capturing machine data, given the often limited lifespan of a container. Container metrics contain details related to CPU, memory, I/O, and network metrics generated by a container. By capturing this data, you have the opportunity to spot specific containers that appear to consume more resources than others – enabling faster, more precise troubleshooting.

Application

Kubernetes

- Monitoring Kubernetes sensitive role activities
- Detecting Kubernetes scanning activity
- Monitoring Kubernetes sensitive object access
- Monitoring Kubernetes pods

Sources

Guidance for onboarding data can be found in the Spunk Documentation, Getting Data In (Splunk Enterprise) or Getting Data In (Splunk Cloud). In addition, these Splunk Add-Ons and Apps are helpful for working with container data.

- Splunk Connect for Docker


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.