Collecting Logs from Linux Servers with Filebeat

Josh Stroschein

Security Researcher

@jstrosch   www.0xevilc0de.com
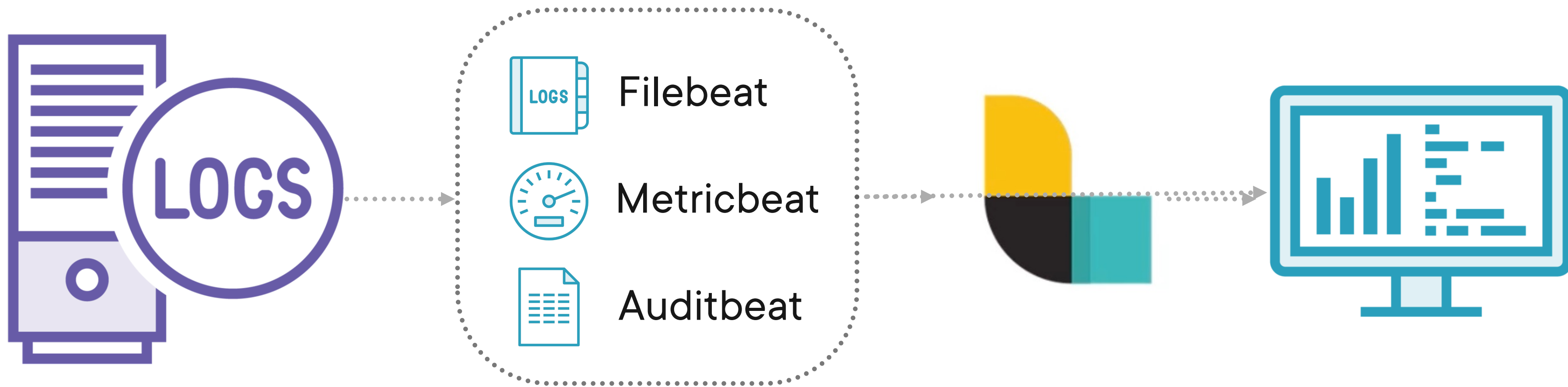
Overview

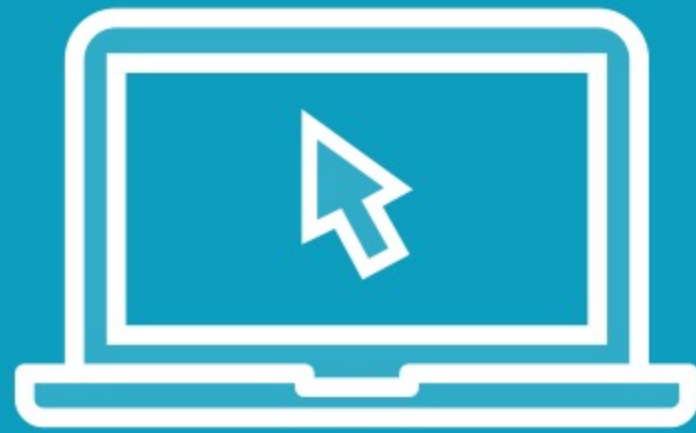**Install Filebeat and Metricbeat on Linux servers**

Setup default dashboards
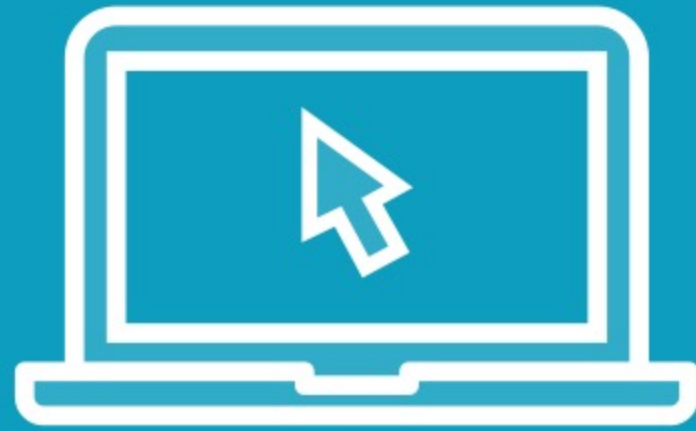
Instrumenting Linux Servers

Filebeat

Metricbeat

Auditbeat

Demo

Install Filebeat in a Linux server

Briefly explore the default dashboards

Demo

Install Metricbeat in a Linux server