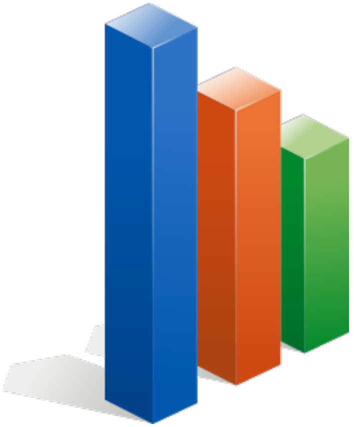
Reporting and Alerting >

- Reports and alerts are knowledge objects in Splunk
- To create reports and alerts, you need a Splunk Enterprise license
  - The free license disables these features



Reporting and Alerting >

Reports

- Saved searches that can run on a schedule and perform an action
    - Send an e-mail to report consumers
    - Embed on a web page
    - Update a dashboard panel
    - Run a script

Reporting and Alerting >

Reports

- Scheduled reports can run
    - Every hour
    - Every day
    - Every week
    - Every month
    - On a chron schedule that you define
- You can stagger the report running window
    - Useful if you have a lot of reports running at the same time

Reporting and Alerting >

Alerts

- Can be scheduled or in real-time
- Triggered when the results of a search meet a specific condition that you define
  - For example, if the search `host=firewall1 user=* authentication=failed` returns anything, trigger an alert

Reporting and Alerting >

Alerts

- Alert actions can include
  - Send an email
  - Trigger a script
  - Use a webhook
  - List in triggered alerts
  - Use an app (like PagerDuty or Slack)

Demo: Reporting and Alerting

Thanks, Splunkers!