SPLUNK EDUCATION

Course Description

Splunk On-Call Administration

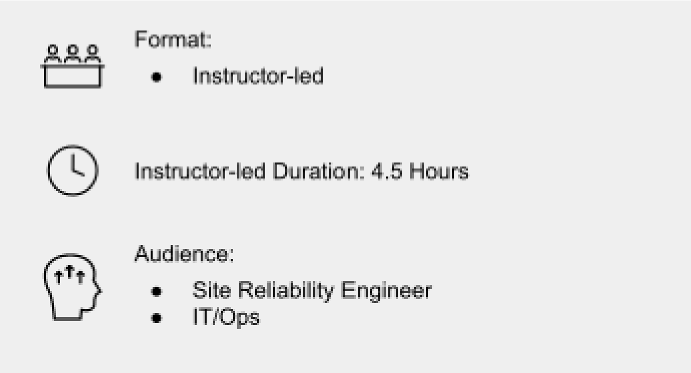
Summary

This course is targeted towards Splunk On-call admins responsible for setting up incident response with Splunk On-Call. This 4.5-hour virtual course describes the tasks required to set up on-call teams, including defining schedules, on-call rotations and shifts. Learn to set-up and configure alerts and integrations. Explore post-incident review reports, track response metrics and customize reports. Use advanced features such as the Rules engine for advanced customization and configure webhook integrations.

Learn the concepts and apply the knowledge through interactive lectures, discussions, and hands-on exercises.

Prerequisites

- Familiar with On-Call



Format:

- Instructor-led

Instructor-led Duration: 4.5 Hours

Audience:

- Site Reliability Engineer
- IT/Ops

Course Outline

Module 1 – Getting Started with Users and Teams

- Describe What Splunk On-Call is
- Describe the flow of an alert/ incident in Splunk On-Call
- Create a plan for incident response
- Describe the layout of the On-Call User Interface
- Create new users and teams
- Create user paging (notification) policies
- Create new Teams
- Add users to teams

Module 2 – Incident Response Through Team Rotations and Escalation Policies

- Create on-call schedules
    - ○ Add rotations
    - ○ Add shifts
    - ○ Add members
- Build escalation policies to handle incidents

Module 3 – Alert Rules Engine

- Create Routing Keys to direct incoming alerts
- Use the Alert Rule Engine to create alert rules
- Use the Alert Rule Engine to transform fields

Module 4 – Integrations

- Select appropriate external Monitoring System integrations
- Configure common Splunk On-Call integrations

Module 5 – Reporting on Team Activity and Performance

- Differentiate between the types of reports
- Create a post-incident review report
- Track response metrics
- Customize on-call Review report
- Track flow of incidents using the Incident Frequency report (Enterprise edition only)

Module 6 – (optional) Advanced Features

- Use Terraform to manage On-Call
- Use Maintenance Mode
- Use Conference Bridge
- Use Alert Configurations

About Splunk Education

With Splunk Education, you and your teams can learn to optimize Splunk through self-paced eLearning and instructor-led training, supported by hands-on labs. Explore learning paths and certifications to meet your goals. Splunk courses cover all product areas, supporting specific roles such as Splunk Platform Search Expert, Splunk Enterprise or Cloud Administrator, SOC Analyst or Administrator, DevOps or Site Reliability Engineer, and more. To learn more about our flexible learning options, full course catalog, and Splunk Certification, please visit http://www.splunk.com/education.

To contact us, email education@splunk.com.