Splunk On-Call Administration

This course is targeted towards Splunk On-call admins responsible for setting up incident response with Splunk On-Call. This 1-virtual day 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. Create 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. All concepts are taught using lectures and scenario-based hands-on activities.

Course Topics

- Set up Splunk On-Call teams
- Set up integrations and configure alerts
- Report on team activity and performance
- Use the Rules engine to trigger custom alerts
- Set up webhook integrations

Course Prerequisites

None

Class Format

Instructor-led lecture with labs, delivered via virtual classroom or at your site

Course Objectives

Module 1 – Introduction and Planning

- Identify features desirable in an incident response system
- Create a plan for incident response
- Describe the flow of a typical incident in Splunk On-Call
- Describe the general layout of the UI / functionality
- Explain the Splunk on-call concepts including: Escalation Policies, Incidents, and Actions
- Create new users
- Create user paging (notification) policies
- Plan on-call schedules

Module 2 – Users, Teams, Rotations and Escalation Policies

- Describe the Splunk On-Call setup flow
- Differentiate between Splunk On-Call user roles
- Create teams and add users using both the UI and API
- Add and remove team managers
- Create on-call schedules including shifts, rotations, and members
- Build Escalation Policies for incoming incidents

Module 3 – Configuring Integrations and Alerts

- Describe the purpose of a routing key
- Explain the importance of naming conventions in creating routing keys and escalation policies.
- Create a routing key
- Select appropriate external Monitoring System integrations
- Configure 3 Splunk On-Call integrations

Module 4 – 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 after the fact using the Incident Frequency report (Enterprise edition only)

Module 5 – Advanced Features

- Use the Alert Rules Engine to add annotations to an incident
- Use the Alert Rules Engine to transform an alert
- Re-route or mute incidents based on content
- Create outgoing Webhooks to extend product functionality
- Use the public API portal to find details on the public API
- Explain what data in Splunk On-Call can be maintained with Terraform

About Splunk Education

Splunk classes are designed for specific roles such as Splunk Administrator, Developer, User, Knowledge Manager, or Architect.

Certification Tracks

Our certification tracks provide comprehensive education for Splunk customer and partner personnel according to their areas of responsibility.

To view all of Splunk Education's course offerings, or to register for a course, go to http://www.splunk.com/goto/education

To contact us, email education_AMER@splunk.com