Splunk On-Call Administration

Category: AI, Data & Analytics | **Vendor:** Splunk

Duration: 8.00 hours (1 days) **6.5 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format: Instructor Led - Online

Course Overview

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.

About This Course

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.

Who Should Attend

- Site Reliability Engineer
- IT/Ops

Prerequisites & Entry Requirements

General Prerequisites:

- Familiar with On-Call

Detailed 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

Frequently Asked Questions

Q: What delivery options are available for Splunk On-Call Administration?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: How many CPD hours does this course provide?

The 1-day Splunk On-Call Administration course provides up to 6.5 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the Splunk On-Call Administration training?

The training takes place over 1 day(s), with each day lasting approximately 8.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for Splunk On-Call Administration?

Yes, we provide corporate training, dedicated training, and closed classes for Splunk On-Call Administration. Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: Splunk On-Call Administration, Splunk Observability, SOCA

Q: Why choose Nexus Human for Splunk On-Call Administration?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your Splunk On-Call Administration training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 XXX XXXX (Ireland) | +44 20 XXXX XXXX (UK)