Using SignalFlow in Splunk Observability Cloud

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

Duration: 16.00 hours (2 days) **13.0 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format: Instructor Led - Online

Course Overview

This 2-day (virtual days) course is targeted towards SREs, ITOps, and DevOps Engineers who are responsible for implementing and maintaining an observability solution for infrastructure and application monitoring. In this advanced technical course, you will learn to use SignalFlow – the analytics language used in Splunk Observability Cloud. SignalFlow is a programming language used to define Charts, Navigators and Detectors, and for more complicated data manipulation.

Use SignalFlow to develop visualizations and detectors that are more specific and reusable than what is possible using the user interface alone. You will create functions to analyze data and to incorporate elements from the Observability Cloud code library. The content covered in this course is essential to managing Observability Cloud resources as code using the REST API, Terraform or another content-as-code solution.

Learn the concepts and apply the knowledge through demonstrations, discussions and hands-on activities.

Note: Much of the content in this course was previously covered in the retired course "Automation and the REST and SignalFlow APIs".

About This Course

This 2-day (virtual days) course is targeted towards SREs, ITOps, and DevOps Engineers who are responsible for implementing and maintaining an observability solution for infrastructure and application monitoring. In this advanced technical course, you will learn to use SignalFlow – the analytics language used in Splunk Observability Cloud. SignalFlow is a programming language used to define Charts, Navigators and Detectors, and for more complicated data manipulation.

Use SignalFlow to develop visualizations and detectors that are more specific and reusable than what is possible using the user interface alone. You will create functions to analyze data and to incorporate elements from the Observability Cloud code library. The content covered in this course is essential to managing Observability Cloud resources as code using the REST API, Terraform or another content-as-code solution.

Learn the concepts and apply the knowledge through demonstrations, discussions and hands-on activities.

Note: Much of the content in this course was previously covered in the retired course "Automation and the REST and SignalFlow APIs".

Prerequisites & Entry Requirements

General Prerequisites:

- Visualizing and Alerting in Splunk Observability Cloud (VASIM)
- Experience working with programming languages such as Python (preferred), JavaScript, or Go.

Note: If you have not worked extensively with Splunk Observability Cloud you should take another course first before continuing with this one.

Learning Outcomes

Upon successful completion of this course, participants will be able to:

- Writing your first SignalFlow program
- Working with Data Streams in Splunk Observability Cloud
- Stream aggregations, transformations, and calculations
- Detecting and alerting in SignalFlow
- Advanced detecting and stream manipulation
- The SignalFlow REST API

Detailed Course Outline

Module 1 – Writing Your First SignalFlow Program

- Identify where SignalFlow is used in Splunk Observability Cloud
- Create plots using SignalFlow instead of the Plot Builder
- Query streaming data
- Add filters to streaming data queries
- Combine filters with and, or, not

Module 2 – Working with Data Streams in Splunk Observability Cloud

- Describe the fundamentals of Data Stream objects
- Use aggregation functions to analyze streaming data
- Apply transformations to streaming data
- Change resolutions, rollups, and extrapolation policies when querying streaming data

Module 3 – Stream aggregations, transformations, and calculations

- Use combining operators on streams
- Operate on data streams with missing data
- Use the map() method to modify or exclude values in a stream
- Describe variable assignment in SignalFlow
- Differentiate between SignalFlow functions and methods
- Describe and use SignalFlow functions that have equivalent methods

Module 4 – Detecting and Alerting in SignalFlow

- Use the detect() function to monitor a stream
- Use comparisons to create Boolean streams
- Create constant streams and use them appropriately
- Specify different "on" and "off" conditions for a detect block
- Identify durations of an occurrence in streaming data
- Compare streams using different thresholds for different MTSs
- Create alerts rules that align with detectors

Module 5 – Advanced Detecting and Stream Manipulation

- Work with properties and dimensions in SignalFlow
- Compare values using multiple thresholds and a default
- Use built-in library functions
- Use conditional, list, and other Python-like functionality
- Write reusable functions in SignalFlow

Module 6 – The SignalFlow REST API

- Explain the SignalFlow APIs available and common use cases
- Execute a SignalFlow program using the HTTP API

- Describe the data format returned by the HTTP API

- Explain how Terraform is used to manage Infrastructure Monitoring resources in Splunk Observability Cloud

- Create detectors and alert rules using the REST API

Skills You Will Learn:

- Writing your first SignalFlow program
- Working with Data Streams in Splunk Observability Cloud
- Stream aggregations, transformations, and calculations
- Detecting and alerting in SignalFlow
- Advanced detecting and stream manipulation
- The SignalFlow REST API

Frequently Asked Questions

Q: What delivery options are available for Using SignalFlow in Splunk Observability Cloud?

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 2-day Using SignalFlow in Splunk Observability Cloud course provides up to 13.0 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the Using SignalFlow in Splunk Observability Cloud training?

The training takes place over 2 day(s), with each day lasting approximately 16.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for Using SignalFlow in Splunk Observability Cloud?

Yes, we provide corporate training, dedicated training, and closed classes for Using SignalFlow in Splunk Observability Cloud. 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: Using SignalFlow in Splunk Observability Cloud, Splunk Observability, AURSAPI

Q: Why choose Nexus Human for Using SignalFlow in Splunk Observability Cloud?

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 Using SignalFlow in Splunk Observability Cloud 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)