Course Code: 6A402G

Course Title: IBM Safer Payments: Hands-on Technical Primer (v6.4.x)

Description:

IBM Safer Payments is an enterprise fraud detection solution. It is a designed and focused on real time payment transaction processing. Safer Payments provides complex and dynamic rules building, evaluation and execution. Built with real time performance, management, and redundancy in mind.

In this course, technical resources that will be involved in any aspect of deploying, customizing, and implementing the Safer Payment solution will get a hands-on overview of the product. Students will get an understanding of how to install, configure, and setup the system for Analysts as well as basics on system administration.

Objectives:

In this course, students will learn about the following:

- Install and configure a Safer Payments cluster (Linux environment)
- Understand how to ingest and map data into Safer Payments
- Understand the cluster architecture of Safer Payments
- Set up Safer Payments for real-time processing of messages
- Manually configure rules including profilings
- Run simulations to test rules
- Set up case investigation to create and investigate alerts

Prerequisites:

- Must be familiar with Unix command line navigation and configuration actions
- Some familiarity with payment processing systems
- Familiarity with the concepts of clustering and network/firewall topics
- Familiarity and comfort with troubleshooting and problem determination processes

Duration:

32 Hrs

Topics:

Day 1: Installation, cluster configuration, and system configuration

- Introductory Overview of Safer Payments
- SP Cluster Architecture (Interfaces and Redundancy)
- Installing Safer Payments
- Mandator Hierarchy
- User Roles and User Accounts

Day 2: Data Dictionary and Batch Data Import

- Revision concept
- Introduction to SP’s data model
- Data storage and retention
- Masterdata
- Data ingestion and data formats
- Merging

Day 3: Modelling in Safer Payments

- Modelling in Safer Payments – An introduction and basic concepts
- Behavior Profiling
- Manually creating rules
- Testing and simulating rules
- Python callouts
- External Modelling
- Sampling

Day 4: Compliance lists, Case Investigation, and Reports

- Rule Generator
- Internal Random Forest
- Compliance Lists
- Defined Risk Lists
- Reports and query functionality
- Case Management and Case Investigation

Audience:

- External: Fraud Analysts, Application and System Admins managing Safer Payments
- Internal: IBM Lab Services, IBM Support, IBM Technical Pre-Sales and IBM BusinessPartners