Course Code: 8G102G

Course Title: IBM Security Guardium Data Protection Foundations

## Description:

IBM Security® Guardium® Data Protection (Guardium) supports a zero trust approach to security. It discovers and classifies sensitive data from across an enterprise, providing real time data activity monitoring and advanced user behavior analytics to help discover unusual activity around sensitive data.

Guardium provides a broad range of data security and protection capabilities that can protect sensitive and regulated data across environments and platforms. This course provides the foundational level processes, procedures, and practices necessary to configure Guardium to monitor and protect sensitive data. Hands-on exercises reinforce the skills learned.

*Note: this course is based upon IBM Security® Guardium® Data Protection v11.4.

## Objectives:

- Identify the primary functions of IBM Security Guardium Data Protection
- Apply key Guardium architecture components
- Navigate the Guardium user interface and command line interface
- Manage user access to Guardium
- Build and populate Guardium groups
- Use system settings and data management tools to manage, configure and monitor Guardium resources
- Use database discovery and the Vulnerability Assessment application to perform data security tasks
- Configure policy rules that process the information gathered from database and file servers
- Create queries and reports to examine trends and gather data
- Use Guardium alerts to monitor a data environment
- Use Guardium audit process tools to streamline the compliance process

## Prerequisites:

Before taking this course, make sure that you have the following skills:

- Working knowledge of SQL queries for IBM DB2 and other databases
- Working knowledge of NoSQL type databases
- Working knowledge of UNIX commands
- Ability to use a UNIX text editor such as vi
- Familiarity with data protection standards such as HIPAA, PCI, GDPR, and SOX

## Duration:

24 Hrs

## Topics:

Unit 1: Guardium overview

Unit 2: Guardium architecture

Unit 3: Guardium user interfaces

Unit 4: Access management

Unit 5: Guardium groups

Unit 6: System & data management

Unit 7: Guardium discovery & vulnerability assessment

Unit 8: Policy management

Unit 9: Guardium reporting

Unit 10: Guardium alerts

Unit 11: Audit process automation

## Audience:

Database administrators, security administrators, security analysts, security technical architects, and professional services using Guardium.