COURSE TABLE OF CONTENTS

IBM Certified Administrator — Security Guardium V11.x

OEM: IBM • Duration: 3 Days (24 hrs) • Code: C1000-127

COURSE MODULES & TOPICS

Section 1: Plan for the IBM Security Guardium System (10%)

- Describe Guardium Architecture
- Define the differences between Guardium agents
- Identify the ports for Guardium and agents
- Define the roles of Guardium appliances (Collector, Aggregator, Central Manager)
- Explain deployment models: Standalone, Distributed, High Availability
- S-TAP and C-TAP deployment considerations

Section 2: Deploy and Configure the IBM Guardium System (13%)

- Configure Guardium appliances
- Install license keys
- Install Guardium agents
- Configure and attach Identity Providers
- Configure SMTP and SIEM on appliance
- Configure user roles and permissions
- Database and OS integrations (GIM, GRD, LDAP/AD)

Section 3: Discover and Classify (7%)

- Discover the databases on the network
- Locate and classify sensitive data
- Data Classification — identifying sensitive data
- Entitlement Reports — user access permissions

Section 4: Protect and Monitor (18%)

- Build a policy
- Define and implement Policy Rules logic
- Setup outlier detection settings
- Differentiate between policy actions
- Interpret results of analytic engines
- Monitor resources of appliance

- Configure database and file activity monitoring
- Customize audit processes
- Using exceptions, filters, and access groups

Section 5: Audit and Report (13%)

- Create custom report queries
- Configure audit flow
- Schedule and export reports
- Compliance frameworks (GDPR, HIPAA, SOX, PCI-DSS)

Section 6: Assess and Harden (7%)

- Identify vulnerabilities in databases and platforms
- Harden vulnerabilities in databases and platforms
- Configure and operate CAS
- Run database vulnerability scans
- Analyze scan results and generate compliance reports
- Remediation tracking (VA, SCAP, CIS Benchmarks)

Section 7: Maintain and Manage (18%)

- Configure high availability functions for appliances and agents
- Configure alerts
- Install patches
- Configure data management
- Manage and maintain groups and user accounts
- SIEM Integration (QRadar, Splunk)
- Incident Response Workflow

Section 8: Problem Determination (14%)

- Troubleshoot installation issues
- Troubleshoot data capture issues
- Troubleshoot operational issues
- Generate must gathers
- Backup and restore procedures
- Log analysis (Guardium logs, OS logs)
- Performance tuning and CLI Troubleshooting