Cloud Data Warehouse Security Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The shift to cloud-native architectures has made Cloud Data Warehouses indispensable for Big Data analytics, machine learning, and business intelligence. However, this migration introduces complex cybersecurity challenges, as sensitive corporate data is now managed across a Shared Responsibility Model in platforms like AWS Redshift, Google BigQuery, and Snowflake. In an era defined by stringent Data Governance mandates like GDPR and HIPAA, and an alarming rise in sophisticated cloud security breaches, traditional security perimeters are obsolete. Organizations urgently require professionals skilled in implementing Zero Trust principles, advanced Data Encryption, and granular Access Control to protect their most critical asset: data.

Cloud Data Warehouse Security Training Course addresses the urgent market demand for specialists in securing modern CDWH environments. Participants will gain hands-on expertise in developing a holistic security posture from ingestion to consumption. The curriculum focuses on practical, platform-agnostic best practices while diving deep into specific vendor capabilities for Identity and Access Management (IAM), Network Security, and Compliance Automation. By mastering DevSecOps integration, Vulnerability Management, and robust Incident Response workflows, graduates will be equipped to architect resilient, secure, and cost-optimized cloud data solutions, transforming them from security liabilities into reliable, confidential business enablers.

Programme Curriculum

Cloud Data Warehouse Security Training Course

Introduction

The shift to cloud-native architectures has made Cloud Data Warehouses indispensable for Big Data analytics, machine learning, and business intelligence. However, this migration introduces complex cybersecurity challenges, as sensitive corporate data is now managed across a Shared Responsibility Model in platforms like

AWS Redshift, Google BigQuery, and Snowflake. In an era defined by stringent Data Governance mandates like GDPR and HIPAA, and an alarming rise in sophisticated cloud security breaches, traditional security perimeters are obsolete. Organizations urgently require professionals skilled in implementing Zero Trust principles, advanced Data Encryption, and granular Access Control to protect their most critical asset: data.

Cloud Data Warehouse Security Training Course addresses the urgent market demand for specialists in securing modern CDWH environments. Participants will gain hands-on expertise in developing a holistic security posture from ingestion to consumption. The curriculum focuses on practical, platform-agnostic best practices while diving deep into specific vendor capabilities for Identity and Access Management (IAM), Network Security, and Compliance Automation. By mastering DevSecOps integration, Vulnerability Management, and robust Incident Response workflows, graduates will be equipped to architect resilient, secure, and cost-optimized cloud data solutions, transforming them from security liabilities into reliable, confidential business enablers.

Course Duration

5 days

Course Objectives

1. Architect and implement a Zero Trust Architecture (ZTA) specifically for multi-cloud data warehouse environments.
2. Master Data Encryption techniques for data at rest and in transit, including Key Management Service (KMS) integration across major clouds.
3. Design and enforce fine-grained Access Control using Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and native platform features.
4. Configure and audit Identity and Access Management (IAM) policies and roles to adhere to the principle of least privilege.
5. Implement robust Network Security controls, including VPC/VNet peering, Private Link, and network segmentation for CDWH isolation.
6. Develop a comprehensive Data Classification and Data Masking strategy for handling sensitive and personally identifiable information (PII).
7. Integrate Security Information and Event Management (SIEM) and Cloud Security Posture Management (CSPM) tools for continuous monitoring and auditing.
8. Formulate and execute Incident Response and Disaster Recovery plans tailored for CDWH breaches and outages.
9. Ensure CDWH solutions achieve and maintain Compliance Automation with industry standards
10. Secure the entire Data Pipeline, from ingestion to consumption, against common threats like SQL Injection.
11. Perform regular Vulnerability Assessment and Configuration Audits on CDWH infrastructure and services.
12. Apply DevSecOps principles to embed security controls directly into the CI/CD pipeline for data infrastructure.
13. Optimize security processes for Cost Management while maintaining a high Security Posture.

Target Audience

1. Cloud Security Engineers/Architects.
2. Data Engineers/Architects.
3. Database Administrators.

4. Security Analysts/Auditors.
5. DevOps/DevSecOps Engineers.
6. Compliance and Governance Professionals.
7. Technical Leaders.
8. IT/Data Consultants.

Course Modules

Module 1: Cloud Data Warehouse Fundamentals and Shared Responsibility

- CDWH and Data Lakehouse, Architectural Overview
- Deep dive into the Shared Responsibility Model for Data Warehouses and its security implications.
- Establishing a framework for sensitive data.
- Securing the account/project level and networking fundamentals
- Case Study: Analyzing a major CDWH misconfiguration breach to identify failed security controls under the shared model.

Module 2: Identity, Access Management (IAM), and Authentication

- Designing and implementing Role-Based Access Control and Attribute-Based Access Control
- Enforcing Multi-Factor Authentication and integrating with enterprise Identity Providers
- Auditing and managing service accounts and privileged access using PIM/PAM best practices.
- Securing API keys, credentials, and access tokens for programmatic access.
- Case Study: Implementing a Zero Trust access policy for an internal BI team using federated identity and conditional access.

Module 3: Data Encryption and Key Management Strategy

- Implementing data at rest encryption
- Securing all data movement with TLS/SSL for ETL/ELT pipelines and BI connections.
- Utilizing and hardening Cloud KMS for key lifecycle management.
- Exploring advanced techniques like secure enclaves for processing highly sensitive data.
- Case Study: Migrating a legacy data warehouse to the cloud, enforcing a Customer-Managed Key encryption strategy, and designing the key rotation policy.

Module 4: Network and Perimeter Security

- Configuring VPC/VNet endpoints and private networking to block public internet access to the data warehouse.
- Implementing fine-grained ingress/egress rules and WAF for web-facing analytics components.
- Utilizing database-specific features for policy-based network control.
- Preventing unauthorized data exfiltration using service control policies.
- Case Study: Hardening a hybrid CDWH deployment by establishing secure VPN tunnels and private endpoints for on-premises ETL agents.

Module 5: Data Privacy, Masking, and Granular Control

- Implementing Row-Level Security and Column-Level Security to restrict visibility of sensitive fields.
- Applying static and dynamic data masking and tokenization for non-production environments and analytics users.
- Configuring comprehensive logging, including query history, access attempts, and administrative actions.

- Setting up DLP policies to detect and block the movement of sensitive data outside permitted boundaries.
- Case Study: Designing and implementing RLS/CLS for a financial services data warehouse to segment customer and regional data access.

Module 6: Compliance, Governance, and Regulatory Frameworks

- Mapping CDWH security configurations to GDPR, HIPAA, and PCI-DSS requirements.
- Utilizing cloud-native and third-party tools to continuously check for misconfigurations and compliance drift.
- Preparation for external audits, demonstrating control effectiveness and log retention policies.
- Conducting regular threat modeling specific to data warehouse workloads and data flows.
- Case Study: Demonstrating a live compliance check using a CSPM tool, identifying a critical violation, and orchestrating the automated remediation.

Module 7: Threat Detection, Incident Response, and Vulnerability

- Forwarding audit and security logs to Splunk, Sentinel, or a central SIEM for correlation and alerting.
- Setting up alerts for unusual data access patterns, privilege escalations, or high-volume data exfiltration attempts.
- Scanning CDWH infrastructure components and implementing a patching strategy.
- Developing and practicing a specific Data Breach Incident Response Plan for a CDWH compromise.
- Case Study: Simulating a supply chain attack and executing the full Incident Response Playbook.

Module 8: DevSecOps and Future-Proofing CDWH Security

- Defining and deploying secure CDWH infrastructure using Terraform or CloudFormation and policy-as-code.
- Integrating security checks directly into the data pipeline deployment process.
- Securing serverless data processing components that interact with the CDWH.
- Understanding and mitigating risks associated with using data warehouse data for AI/ML model training.
- Case Study: Automating the deployment of a new, secure data warehouse environment using IaC and validating the security posture with automated tests.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.com or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to FINESKILL TRAINING CENTER account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
07 Sep 2026	11 Sep 2026	Online	$1,100
14 Sep 2026	18 Sep 2026	Online	$1,100
21 Sep 2026	25 Sep 2026	Online	$1,100
28 Sep 2026	02 Oct 2026	Online	$1,100
05 Oct 2026	09 Oct 2026	Online	$1,100
12 Oct 2026	16 Oct 2026	Online	$1,100
19 Oct 2026	23 Oct 2026	Online	$1,100
26 Oct 2026	30 Oct 2026	Online	$1,100

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now