AWS Security Governance at Scale

Course Content

Course Description:

In this course, you will learn how security is foundational to AWS. Governance at scale is a new concept for automating cloud governance that can help companies retire manual processes in account management, budget enforcement, and security and compliance. By automating common challenges, companies can scale without inhibiting agility, speed, or innovation. In addition, they can provide decision makers with the visibility, control, and governance necessary to protect sensitive data and systems. In this course, you will learn how to facilitate developer speed and agility, and incorporate preventive and detective controls. By the end of this course, you will be able to apply governance best practices.

Course Objectives:

In this course, you will learn to:
- Establish a landing zone with AWS Control Tower
- Configure AWS Organizations to create a multi-account environment
- Implement identity management using AWS Single Sign-On users and groups
- Federate access using AWS SSO
- Enforce policies using prepackaged guardrails
- Centralize logging using AWS CloudTrail and AWS Config
- Enable cross-account security audits using AWS Identity and Access Management (IAM)
- Define workflows for provisioning accounts using AWS Service Catalog and AWS Security Hub

Prerequisites:

AWS Security Fundamentals
AWS Security Essentials

Target Audience:

This course is intended for:
- Solutions architects, security DevOps, and security engineers

Topics:

Lesson 1: Governance at Scale
- Governance at scale focal points
- Business and Technical Challenges

Lesson 2: Governance Automation
- Multi-account strategies, guidance, and architecture
- Environments for agility and governance at scale
- Governance with AWS Control Tower
- Use cases for governance at scale

Lesson 3: Preventive Controls
- Enterprise environment challenges for developers
- AWS Service Catalog
- Resource creation
- Workflows for provisioning accounts
- Preventive cost and security governance
- Self-service with existing IT service management (ITSM) tools

Lab 1: Deploy Resources for AWS Catalog
- Create a new AWS Service Catalog portfolio and product
- Add an IAM role to a launch constraint to limit the actions the product can perform.
- Grant access for an IAM role to view the catalog items
- Deploy an S3 bucket from an AWS Service Catalog product

Lesson 4: Detective Controls
- Operations aspect of governance at scale
- Resource monitoring
- Configuration rules for auditing
- Operational insights
- Remediation
- Clean up accounts

Lab 2: Compliance and Security Automation with AWS Config
- Apply Managed Rules through AWS Config to selected resources
- Automate remediation based on AWS Config rules
- Investigate the Amazon Config dashboard and verify resources and rule compliance

Lab 3: Taking Action with AWS Systems Manager
- Setup Resource Groups for various resources based on common requirements
- Perform automated actions against targeted Resource Groups

Lesson 5: Resources
- Explore additional resources for security governance at scale

Register for this class by visiting us at:
www.tcworkshop.com or calling us at 800-639-3535