AWS Security Live Training Sample Agenda

1. Using IAM for User and Group Permissions (0.5 hours)
    a. Overview
    b. Interactive Labs
        i. Log into AWS account
        ii. Configure users and permissions
    c. Challenge
        i. Set up Multi-factor Authentication (MFA)
2. Security of Core AWS Resources (1 hour)
    a. Overview
    b. Interactive Labs
        i. Configure a VPC with a public and private subnet
        ii. Access EC2 instance in private subnet
    c. Challenge:
        i. Provision a NAT Gateway
3. Accessing AWS Resources from EC2 (1 hour)
    a. Overview
    b. Interactive Labs
        i. Access S3 from an EC2 instance
        ii. Configure IAM roles and policies
    c. Challenge:
        i. Use KMS encryption to lock down access to S3
4. Provision and Configure Security on Real-World Architectures (1.5 hours)
    a. Overview
    b. Interactive Labs
        i. Deploy a Serverless website
        ii. Deploy a WordPress application
        iii. Set up a Web Application Firewall (WAF)

LUNCH BREAK (0.5 hours)

5. Operational Monitoring (1.5 hours)
    a. Overview
    b. Interactive Labs
        i. Set up automated security response that emails you whenever a user logs in
        ii. Set up AWS Config to detect public S3 buckets
6. Managed Security Services (1 hour)
    a. Overview
    b. Interactive Labs
        i. Run a scan with Amazon Inspector