Security Engineering on AWS

AWS クラスルームトレーニング

コースの説明

AWS セキュリティサービスを使用して、AWS クラウドで安全な環境を維持する方法について学習します。AWS が推奨するセキュリティプラクティスを使用して、クラウド内のデータとシステムのセキュリティを強化します。このコースでは、コンピューティング、ストレージ、ネットワーキング、データベースといった AWS のキーサービスのセキュリティ機能に注目します。また、AWS の各サービスとツールを活用して、継続的なモニタリングとログ記録、セキュリティインシデントへの対応を行う方法についても学びます。

レベル	実施形式	所要時間
中級	クラスルームトレーニング、ハンズオンラボ	3 日間

コースの目標

このコースの学習内容は、以下のとおりです。

- AWS の責任共有モデルを習得する
- よく見られるセキュリティ上の脅威から保護した AWS アプリケーションインフラストラクチャを設計、構築する
- 保管中のデータおよび転送中のデータを暗号化して保護する
- セキュリティチェックと分析を再現可能な方法で自動的に適用する
- AWS クラウドでリソースおよびアプリケーションの認証を設定する
- ログを記録、モニタリング、処理、分析してイベントの詳細を確認する
- アプリケーションおよびデータに侵入してきた脅威を特定し、軽減する
- セキュリティ評価を実施して、一般的な脆弱性が修復されており、セキュリティ面のベストプラクティスが実施されていることを確認する

対象者

このコースは以下のような方を対象としています。

- セキュリティエンジニア

aws training and certification

Security Engineering on AWS

AWS クラスルームトレーニング

- セキュリティアーキテクト
- 情報セキュリティのプロフェッショナル

前提条件

このコースを受講するにあたっては、次のことを身につけておくことをお勧めします。

- IT セキュリティプラクティスおよびインフラストラクチャの概念の実務的知識
- クラウドコンピューティングの概念に関する知識があること
- AWS Cloud Practitioner Essentials(Second Edition) の無料デジタルコース または クラスルームコース 、 AWS Security Fundamentals デジタルトレーニング 、 Architecting on AWS クラスルームトレーニングの受講

登録

https://www.aws.training/training/schedule?courseId=10021&countryName=JP&trainingProviderId=1

コースの概要

1 日目

モジュール 0: コースの紹介

モジュール 1: セキュリティの概要

- AWS クラウドのセキュリティ
- 責任共有モデル
- 脅威モデリング

モジュール 2: AWS におけるアクセスと権限付与

- AWS を操作するさまざまな方法
- 多要素認証 (MFA) を使用して保護を強化する
- ルートユーザーとアクセスキーを保護する
- IAM ポリシー、ロール、許可の境界
- AWS CloudTrail を使用して API リクエストをログに記録する
- ハンズオンラボ 1: アイデンティティ & リソースベースポリシーの利用

Security Engineering on AWS

AWS クラスルームトレーニング

モジュール 3: AWS におけるアカウント管理とプロビジョニング

- AWS Organizations と AWS Control Tower を使用して複数の Amazon Web Services (AWS) アカウントを管理する方法
- AWS Control Tower でマルチアカウント環境を実装する方法を説明する
- AWS IAM Identity Center (AWS Single Sign-On の後継) と AWS Directory Service の使い方を説明する
- ID プロバイダーとブローカーを使用して Amazon Cognito などの AWS サービスへのアクセスを取得できることを実証する
- 「フェデレーティッド・ユーザー」という用語を定義する
- ハンズオンラボ 2: AWS Directory Service によるドメインユーザーアクセスの管理

2 日目

モジュール 4: AWS でのキーとシークレットの管理

- AWS Key Management Service (AWS KMS)、AWS CloudHSM、AWS Certificate Manager(ACM)、および AWS Secrets Manager の機能について説明し、リストアップする
- マルチリージョン AWS KMS キーを作成する方法をデモする
- AWS Secrets Manager のシークレットを AWS KMS キーで暗号化する方法をデモする
- 暗号化されたシークレットを使用して複数の AWS リージョンの Amazon Relational Database Service (Amazon RDS) データベースに接続する方法を示す
- ハンズオンラボ 3: AWS KMS を使用して Secrets Manager Secrets を暗号化する

モジュール 5: データセキュリティ

- Amazon Macie を使用して機密情報のデータを監視する
- 暗号化とアクセス制御によって保存中のデータを保護する方法を説明する
- 保護のためにデータの複製に使用されている Amazon Web Services (AWS) のサービスを特定する
- アーカイブ後のデータを保護する方法を決定する
- ハンズオンラボ 4: Amazon S3 のデータセキュリティ

モジュール 6: インフラストラクチャとエッジ保護

- 安全なインフラストラクチャを構築するために使用される Amazon Web Services (AWS) 機能について説明する
- 攻撃時の回復力を高めるために使用される AWS サービスについて説明する
- 外部の脅威からワークロードを保護するために使用される AWS サービスを特定する
- AWS Shield と AWS Shield Advanced の機能を比較する

- AWS Firewall Manager を一元的にデプロイすることでセキュリティを強化する方法を説明する
- ハンズオンラボ 5: AWS WAF を使用して悪意のあるトラフィックを軽減する

3 日目

モジュール 7: AWS におけるログのモニタリングと収集

- ログの生成と収集の価値を見極める
- Amazon Virtual Private Cloud (Amazon VPC) フローログの機能を適用してセキュリティイベントをモニタリングする
- ベースラインからの逸脱をモニタリングする方法を説明する
- Amazon Event Bridge のイベントについて説明する
- Amazon CloudWatch メトリクスとアラームについて説明する
- ログ分析オプションと利用可能な手法を一覧で提示する
- Amazon Virtual Private Cloud (VPC) トラフィックミラーリングのユースケースを特定する
- ハンズオンラボ 6: セキュリティインシデントのモニタリングと対応

モジュール 8: 脅威への対応

- インシデント対応でインシデントタイプを分類する
- インシデント対応のワークフローを理解する
- Amazon Web Services (AWS) のサービスを使用してインシデント対応のための情報源を見つける
- インシデントに備える方法を理解する
- AWS のサービスを使用して、脅威 (悪意のある、または不正な行動) を検出する
- セキュリティ上の調査結果を分析して対応する
- ハンズオンラボ 7: インシデント対応