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、オートメーション、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、グループ演習	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 の共有セキュリティ責任モデルを使用する
- 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を使用して保護する
- 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: AWS のセキュリティ

- AWS クラウドのセキュリティ
- AWS の責任共有モデル
- インシデント対応の概要
- DevOps とセキュリティエンジニアリング

モジュール 2: AWS のエントリポイントを確認する

- AWS プラットフォームにアクセスするためのさまざまな方法を確認する
- IAM アクセスキーを保護する方法を説明する
- IAM ポリシーがどのように構築及び設計されているかを分析する
- IAM アクセス許可の境界
- CLI および API によって AWS のエントリポイントを保護する

Security Engineering on AWS

AWS クラスルームトレーニング

- 不審なアクティビティについてアクセス及びユーザー情報を分析する
- ハンズオンラボ 1: クロスアカウントアクセス

モジュール 3: セキュリティに関する考慮事項: ウェブアプリケーション環境

- AWS ウェブアプリケーション環境について説明する
- 3 層アプリケーションを分析し、一般的な脅威を確認する
- 環境評価を実行してセキュリティを強化する

モジュール 4: アプリケーションのセキュリティ

- Amazon EC2 インスタンスと、そのアプリケーションを保護する
- Amazon Inspector を使用して脆弱性を評価する
- AWS Systems Manager を使用してインスタンスにセキュリティチェックを自動的に適用する
- ハンズオンラボ 2: AWS Systems Manager と Amazon Inspector を使用する

モジュール 5: データセキュリティ

- 暗号化とアクセスコントロールによって保管中のデータを保護する方法について説明する
- データ保護のためのレプリケーションに使用する AWS のサービスを特定する
- アーカイブされたデータを保護する方法を決定する

2 日目

モジュール 6:ネットワーク通信を保護する

- セキュリティのベストプラクティスを Amazon VPC に適用する
- 複数の VPC 間で AWS リソースに安全にアクセスする
- インターネットを経由せずに、AWS の他のサービスにプライベート接続する
- 防御ポイントとして Elastic Load Balancing(ELB) を実装する
- パブリック証明書やプライベート証明書を使用して転送中のデータを保護する

モジュール 7: AWS でログをモニタリングし、収集する

- Amazon CloudWatch を使用して AWS クラウドでイベントをモニタリングしログを収集する
- AWS Config を使用してコンプライアンス違反および安全でないリソースをモニタリングする
- Amazon Macie で機密情報のデータをモニタリングする
- ログを生成して収集する AWS ネイティブのサービスを特定する
- Amazon S3 サーバーのアクセスログ
- ELB アクセスログ

- ハンズオンラボ 3 : AWS Lambda と AWS Config を使用したモニタリングと応答

モジュール 8: AWS でログを処理する

- 詳細な分析および可視化のためにログをストリーミングして処理する
- Amazon S3 バケットから直接ログを処理するための AWS のサービスを特定する
- ハンズオンラボ 4 : ウェブサーバーログの分析

モジュール 9: セキュリティに関する考慮事項:ハイブリッド環境

- オンプレミスから AWS への接続に使用される AWS のサービスを
  いくつか特定し、そのセキュリティ機能について説明する
- オンプレミスと AWS の間の転送中にデータを保護する方法を説明する

モジュール 10: リージョン外の保護

- サービス拒否 (DoS) に関する一般的な脅威を特定し分析する
- Amazon Route 53 を使用して攻撃を隔離する方法について説明する
- AWS WAF を実装して不正なトラフィックからウェブアプリケーションを保護する
- Amazon CloudFront を使用してお客様に安全にコンテンツを配信する
- AWS Shield でウェブアプリケーションを保護する

3 日目

モジュール 11: セキュリティに関する考慮事項: サーバーレス環境

- Amazon Cognito を使用して、ウェブ ID プロバイダー経由でユーザーを承認する
- Amazon API Gateway を使用して API のアクセスを制御し、検証する
- AWS Lambda 関数を保護する

モジュール 12: 脅威検出と調査

- スレッドや悪意のある動作、あるいは不正な動作を継続的にモニタリングする
- AWS のサービスおよびパートナー製品全体でセキュリティの検出結果を収集し、優先順位を付ける
- セキュリティの検出結果を調査、分析する

モジュール 13: AWS での機密情報管理

- AWS KMS を使用してキーとデータの暗号化を管理する
- AWS CloudHSM を使用してキーを生成し、保護する方法を説明する

- AWS Secrets Manager を使用してアプリケーションを認証する
- ハンズオンラボ 5: AWS KMS の使用

モジュール 14: 自動化と設計によるセキュリティ

- 「設計による AWS セキュリティ」アプローチを説明する
- 再現可能な方法でセキュリティ指向の AWS 環境をデプロイする
- セルフサービス方式でエンドユーザーが IT サービスを管理および制御できるようにする
- ハンズオンラボ 6: AWS Service Catalog を使用した AWS でのセキュリティのオートメーション

モジュール 15: AWS でのアカウント管理とプロビジョニング

- AWS Organizations を使用して複数のアカウントを一元管理する
- AWS Control Tower を使用してマルチアカウント環境を自動的にデプロイする
- ID プロバイダー/ブローカーを使用して、AWS のサービスにアクセスする
- ハンズオンラボ 7: ADFS を使用したフェデレーションアクセス