Security Engineering on AWS

AWS 課堂培訓

課程說明

對於雲端中的客戶以及考慮採用雲端的客戶而言，安全性都是關注的問題。 對於大多數行業人員來說，網絡攻擊和數據洩漏的增加仍然是首要考慮的。 AWS 上的安全工程課程可協助您更了解如何以安全的方式與 Amazon Web Services (AWS) 互動和建置，以解決這些問題。 在本課程中，您將學習如何管理身分識別和角色、管理和佈建帳戶，以及監控異常情況的 API 活動。 您也將了解如何保護存放在 AWS 上的資料。 本課程將探討如何產生、收集和監控記錄檔，以協助識別安全性事件。 最後，您將檢閱使用 AWS 服務偵測和調查安全事件。

- 課程級別：中級
- 持續時間：3 天

活動

本課程包括簡報、實作手實驗室、示範和小組練習。

課程目標

在本課程中，您將學習：

- 根據 CIA 三元組提出對 AWS 雲端安全的了解。
- 使用 IAM 建立和分析身份驗證和授權。
- 使用適當的 AWS 服務在 AWS 上管理和佈建帳戶。
- 識別如何使用 AWS 服務管理機密。
- 透過加密和存取控制來監控敏感資訊並保護資料。
- 識別可解決外部來源攻擊的 AWS 服務。
- 監控、產生及收集記錄。
- 識別安全事件的指標。
- 識別如何使用 AWS 服務調查威脅和緩解。

Security Engineering on AWS

AWS 課堂培訓

目標受眾

本課程適用於：

- 安全工程師
- 安全建築師
- 雲端架構師
- 跨所有全球細分市場工作的雲運營商

前提

我們建議參加本課程的參加者：

- 完成以下課程：
    - *AWS 安全基本要點* (課堂培訓) 或
    - AWS 安全基礎知識 (第二版) (數位) 和
    - *在 AWS 上建構* (課堂培訓)
- IT 安全實踐和基礎架構概念的工作知識。
- 熟悉 AWS 雲端

課程大綱

第一天

單元 0：AWS 上的安全工程

單元 1：安全性概述

- 說明 AWS 雲端中的安全性。
- 說明 AWS 共同的責任模型。
- 總結 IAM、資料保護以及威脅偵測與回應。
- 使用主控台、CLI 和開發套件陳述與 AWS 互動的不同方式。
- 描述如何使用 MFA 以獲得額外保護。

- 說明如何保護 root 使用者帳戶和存取金鑰。

單元 2：AWS 上的存取和授權

- 說明如何使用多重要素驗證 (MFA) 來提供額外保護。
- 說明如何保護 root 使用者帳戶和存取金鑰。
- 說明 IAM 政策、角色、政策元件和權限界限。
- 說明如何使用 AWS CloudTrail 記錄和檢視 API 請求，以及如何檢視和分析存取歷史記錄。
- 實作實驗室：使用身分識別和資源型原則。

單元 3：AWS 上的帳戶管理和佈建

- 說明如何使用 AWS 組織和 AWS Control Tower 管理多個 AWS 帳戶。
- 說明如何使用 AWS Control Tower 實作多帳戶環境。
- 展示使用身分供應商和代理程式取得 AWS 服務存取權的能力。
- 說明 AWS IAM 身分中心 (AWS 單一登入的繼任者) 和 AWS 目錄服務的使用方式。
- 展示使用目錄服務和 IAM 身分中心管理網域使用者存取的能力。
- 實作實驗室：使用 AWS 目錄服務管理網域使用者存取

第二天

單元 4：在 AWS 上管理金鑰和機密

- 說明並列出 AWS KMS、CloudHSM、AWS Certificate Manager (ACM) 和 AWS Secrets Manager 的功能。
- 示範如何建立多區域 AWS KMS 金鑰。
- 示範如何使用 AWS KMS 金鑰加密密碼管理員密碼。
- 示範如何使用加密密碼連線至多個 AWS 區域中的 Amazon Relational Database Service (Amazon RDS) 資料庫
- 實作實驗室：實驗室 3：使用 AWS KMS 加密機密管理員中的密碼

單元 5：資料安全

- 使用 Amazon Macie 監控敏感資訊的資料。
- 說明如何透過加密和存取控制來保護靜態資料。

- 識別用於複寫資料以進行保護的 AWS 服務。
- 決定封存資料後如何保護資料。
- 實作實驗室：實驗室 4：Amazon S3 中的資料安全

單元 6：基礎架構與邊緣防護

- 描述用於建立安全基礎設施的 AWS 功能。
- 描述在攻擊期間用於建立彈性的 AWS 服務。
- 識別用於保護工作負載免受外部威脅的 AWS 服務。
- 比較 AWS Shield 和 AWS Shield 進階的功能。
- 說明 AWS 防火牆管理員的集中式部署如何增強安全性。
- 實作實驗室：實驗室 5：使用 AWS WAF 防範惡意流量

第三天

單元 7：在 AWS 上監控和收集日誌

- 識別產生和收集記錄檔的值。
- 使用 Amazon Virtual Private Cloud (Amazon VPC) 流程日誌來監控安全事件。
- 說明如何監控基準線偏差。
- 描述 Amazon EventBridge 活動。
- 說明指標和警示。
- 列出日誌分析選項和可用的技術。
- 識別使用 Amazon EventBridge (VPC) 流量鏡像的使用案例。
- 實作實驗室：實驗室 6：監控和回應安全性事件

單元 8：回應威脅

- 在事件回應中分類事件類型。
- 瞭解事件回應工作流程。
- 使用 AWS 服務探索事件回應的資訊來源。
- 瞭解如何為事件做好準備。
- 使用 AWS 服務偵測威脅。

- 分析並回應安全發現項目。
- 實作實驗室：實驗室 7：事件回應

單元 9：AWS 上的安全工程課程總結