Security Engineering on AWS (Simplified Chinese)

AWS 课堂培训

课程说明

无论是已在使用云的客户，还是正在考虑采用云的客户，都会特别关注安全问题。对于业界大多数从业人员来说，网络攻击和数据泄露事件日益频发，一直让他们惴惴不安。Security Engineering on AWS 课程旨在帮助您更好地了解如何以安全的方式使用 Amazon Web Services (AWS) 进行构建并与之交互，有效解决上述问题。在本课程中，您将学习如何管理身份和角色、管理并预置账户，以及监控 API 活动是否存在异常。您还将学习如何保护存储在 AWS 上的数据。本课程将探讨如何生成、收集和监控日志以帮助识别安全事件。最后，您将深入了解如何使用 AWS 服务检测和调查安全事件。

课程级别	授课方式	时长
中级	讲解、动手实验、演示和小组练习	3 天

课程目标

在本课程中，您将学习如何：

- 阐述基于 CIA 三要素的 AWS 云安全性。
- 使用 IAM 创建并分析身份验证和授权。
- 使用适当的 AWS 服务管理和预置 AWS 上的账户。
- 确定如何使用 AWS 服务管理 Secret。
- 通过加密和访问控制监控敏感信息并保护数据。
- 确定可应对从外部源发起的攻击的 AWS 服务。
- 监控、生成和收集日志。
- 识别安全事件指标。
- 确定如何使用 AWS 服务调查和减轻威胁。

目标受众

本课程面向：

- 安全工程师
- 安全架构师

Security Engineering on AWS (Simplified Chinese)

AWS 课堂培训

- 云架构师
- 在所有全球细分市场开展业务的云运营商

先决条件

我们建议符合以下条件的人员参加本课程：

- 已完成以下课程：
    - *AWS Security Essentials*（课堂培训）或
    - AWS Security Fundamentals（第二版）（数字化培训）和
    - *Architecting on AWS*（课堂培训）
- 具备 IT 安全实践和基础设施概念的应用知识。
- 熟悉 AWS 云。

课程大纲

第 1 天

模块 0：**Security Engineering on AWS**

模块 1：安全概览

- 介绍 AWS 云中的安全性。
- 介绍 AWS 责任共担模式。
- 概述 IAM、数据保护以及威胁检测和响应。
- 说明使用控制台、CLI 和 SDK 与 AWS 交互的不同方式。
- 描述如何使用 MFA 实现额外保护。
- 说明如何保护根用户账户和访问密钥。

模块 2：**AWS** 上的访问和授权

- 描述如何使用多重身份验证 (MFA) 实现额外保护。
- 描述如何保护根用户账户和访问密钥。
- 描述 IAM 策略、角色、策略组件和权限边界。
- 说明如何使用 AWS CloudTrail 记录和查看 API 请求，以及如何查看和分析访问历史记录。
- 动手实验：使用基于身份的策略和基于资源的策略

模块 3：**AWS** 上的账户管理和预置

- 说明如何使用 AWS Organizations 和 AWS Control Tower 管理多个 AWS 账户。
- 说明如何使用 AWS Control Tower 实施多账户环境。

Security Engineering on AWS (Simplified Chinese)

AWS 课堂培训

- 展示利用身份提供商和代理获取 AWS 服务访问权限的能力。
- 说明 AWS IAM Identity Center（AWS Single Sign-On 的接替版本）和 AWS Directory Service 的用途。
- 展示使用 Directory Service 和 IAM Identity Center 管理域用户访问的能力。
- 动手实验：使用 AWS Directory Service 管理域用户访问

第 2 天

模块 **4**：在 **AWS** 上管理密钥和 **Secret**

- 描述并列举 AWS KMS、CloudHSM、AWS Certificate Manager (ACM) 和 AWS Secrets Manager 的功能。
- 展示如何创建多区域 AWS KMS 密钥。
- 展示如何使用 AWS KMS 密钥加密 Secrets Manager Secret。
- 展示如何使用加密 Secret 连接到多个 AWS 区域中的 Amazon Relational Database Service (Amazon RDS) 数据库。
- 动手实验：试验 **3 -** 使用 AWS KMS 在 Secrets Manager 中加密 Secret

模块 **5**：数据安全性

- 使用 Amazon Macie 监控数据中的敏感信息。
- 描述如何通过加密和访问控制保护静态数据。
- 确定用于复制数据以实现保护的 AWS 服务。
- 确定如何在数据归档后保护数据。
- 动手实验：实验 **4 -** Amazon S3 中的数据安全性

模块 **6**：基础设施和边缘保护

- 描述用于构建安全基础设施的 AWS 功能。
- 描述用于建立受攻击期间弹性的 AWS 服务。
- 确定用于保护工作负载免受外部威胁的 AWS 服务。
- 比较 AWS Shield 和 AWS Shield Advanced 的功能。
- 说明 AWS Firewall Manager 的集中部署如何增强安全性。
- 动手实验：实验 **5 -** 使用 AWS WAF 减少恶意流量

第 3 天

模块 **7**：在 **AWS** 上监控和收集日志

- 确定生成和收集日志的价值。
- 使用 Amazon Virtual Private Cloud (Amazon VPC) 流日志监控安全事件。
- 说明如何监控基准偏差。
- 描述 Amazon EventBridge 事件。
- 介绍 Amazon CloudWatch 指标和警报。
- 列出日志分析选项和可用的技术。
- 确定使用 Virtual Private Cloud (VPC) 流量镜像的使用案例。
- 动手实验：实验 **6 -** 监控和响应安全事件

Security Engineering on AWS (Simplified Chinese)

AWS 课堂培训

模块 **8**：应对威胁

- 在事件响应中对事件类型进行分类。
- 了解事件响应工作流。
- 使用 AWS 服务查找事件响应的信息来源。
- 了解如何做好应对事件的准备。
- 使用 AWS 服务检测威胁。
- 分析安全调查结果并做出响应。
- 动手实验：实验 **7 -** 事件响应

模块 **9**：**Security Engineering on AWS** 课程总结