Security Engineering on AWS

描述

Security Engineering on AWS 说明了如何高效使用 AWS 安全服务来确保 AWS 云中的安全性和合规性。本课程重点介绍了 AWS 建议的最佳安全实践，您可以通过实施这些最佳实践来增强云中数据和系统的安全性。本课程重点讲解了关键 AWS 服务（包括计算、存储、联网和数据库服务）的安全功能。此外，本课程还介绍了常见的安全控制目标和法规遵从性标准，并分析了在全球不同行业内基于 AWS 运行管制工作负载的使用案例。在本课程中，您还可以了解如何利用 AWS 服务和工具实施自动化及执行持续监控，从而将安全操作提升至更高级别。

级别	授课方式	时长
中级	讲师指导、现场授课或通过虚拟课堂授课	3 天

课程目标

通过学习本课程，您将能够：

- 理解并利用 AWS 共享安全责任模式。
- 在 AWS 云中执行用户身份和访问管理。
- 使用 AWS 安全服务，如 AWS Identity and Access Management、Amazon Virtual Private Cloud、AWS Config、AWS CloudTrail、AWS Key Management Service、AWS CloudHSM 和 AWS Trusted Advisor。
- 对 AWS 云中的资源执行更有效的安全控制。
- 从安全角度管理和审核您的 AWS 资源。
- 监控并记录对 AWS 计算、存储、联网和数据库服务的访问和使用。
- 理解并利用 AWS 共享合规责任模式。
- 确定可用于对 AWS 中的安全操作实施自动化、监控和管理的 AWS 服务和工具。
- 在 AWS 云中执行安全事件管理。

目标人群

本课程适用于：

- 安全工程师
- 安全架构师
- 安全分析师

- 安全审核人员
- 负责监管、审核和测试组织机构的 IT 基础设施并确保该基础设施符合安全、风险和合规性准则的人员

先决条件

我们建议参加学习本课程的人员符合以下先决条件：

- 参加学习过 AWS 安全基础知识
- 在监管、风险及合规规定和控制目标方面有一定经验
- 明白如何应用 IT 安全实践
- 了解 IT 基础设施概念应用方面的知识
- 熟悉云计算概念

授课方式

本课程将结合以下方式授课：

- 讲师指导培训 (ILT)
- 动手实验室

课程大纲

第 1 天

- 模块 1：云安全简介
- 模块 2：云感知监管和合规性
- 模块 3：Identity and Access Management
- 实验 1：使用 AWS IAM
- 模块 4：保护 AWS 基础设施服务 – 第 1 部分
- 实验 2：创建 Virtual Private Cloud

第 2 天

- 模块 5：保护 AWS 基础设施服务 – 第 2 部分
- 模块 6：保护 AWS 容器服务 – 第 1 部分
- 模块 6：保护 AWS 容器服务 – 第 2 部分
- 实验 3：使用 RDS 安全组
- 模块 7：保护 AWS 抽象化服务
- 实验 4：保护 Amazon S3 存储桶
- 模块 8：使用 AWS 安全服务 – 第 1 部分
- 实验 5：捕获日志

第 3 天

- 模块 9：使用 AWS 安全产品 – 第 2 部分
- 实验 6：使用 AWS Config
- 实验 7：使用 AWS Service Catalog
- 模块 10：AWS 云中的数据保护
- 模块 11：基于 AWS 构建合规工作负载 – 案例研究
- 模块 12：云中的安全事件管理