AKAMAI WEB APPLICATION AND API PROTECTION

Course Overview and Agenda

March 2023

Course Overview

The Akamai Web Application and API Protection is a comprehensive course that focuses on configuring and maintaining App & API Protector (AAP) with Advanced Security Management (ASM) using the new Adaptive Security Engine. The course starts with setting up a basic configuration utilizing default best practices. It describes the concepts involved in analyzing and tuning the configuration to maintain it. The participants learn how to protect both APIs and web applications. They are also taught how to detect bots and apply actions to those that pose an immediate threat with the new Bot Visibility & Mitigation (BVM) feature.

The topics presented introduce theoretical knowledge complemented with a suitable hands-on component (eg: a group activity or a lab). The course also outlines common use cases for enhanced user experience.

Objectives

At the end of this course, participants will be able to:

- Describe the basics of the Akamai Intelligent Edge Platform.
- Explain the Threat Landscape as it applies to Web Application Security.
- Describe the features of the Application & API Protection products.
- Configure and activate AAP.
- Test the AAP configuration for APIs and web applications.
- Analyze the behavior of the configuration using reporting and alerting tools.
- Tune AAP in accordance with the results of the analysis.
- Discover the DevOps capabilities using our Security APIs.

Agenda

The Akamai Web Application and API Protection course curriculum can be delivered either as:

- CLASSROOM TRAINING: 2 day (8 hours)
- ONLINE TRAINING: 3 days (4,5 hours each)

The agenda for this training is listed below.

Duration (min)	Module Name & Description
30	**MODULE 1: INTRODUCTION** This module is an introduction to Akamai, the Cloud Security Solutions portfolio, and the Akamai Control Center.
30	**MODULE 2: THREAT LANDSCAPE AND WEB APPLICATION SECURITY** This module will cover the basics of Web Application Security, such as OWASP, common attack trends, and how bots are designed, developed and used to attack web applications.
60	**MODULE 3: SITE DELIVERY COMPONENTS** This module will describe the components used in basic site delivery like Site Shield, Site Failover, Compliance Management, etc. and how they can be edited to optimize the configuration and provide elements of security within the delivery configuration. **LAB: CREATING A DELIVERY CONFIGURATION** **LAB: OPTIMIZING A DELIVERY CONFIGURATION**
30	**MODULE 4: INTRODUCING AAP-ASM** This module will introduce the new App & API Protector (AAP) with Advanced Security Management using the new Adaptive Security Engine, discuss the differences between AAP-ASM and Kona Site Defender or Web Application Protector, and how to upgrade into AAP-ASM from an existing product.
150	**MODULE 5: SECURITY CONFIGURATION** This module discusses the new features of the App & API Protector (AAP) with Advanced Security Management, and how to configure the various components such as Selected Hosts and Match Targets, Rate Controls, Application Layer Controls, Network Layer Controls, and Slow POST protection. **LAB: SETTING UP A SECURITY CONFIGURATION**
60	**MODULE 6: PROTECTING API TRAFFIC** This module focuses on the details of API protection and how to set up a configuration for the protection of APIs.
30	**MODULE 7: CLIENT REPUTATION** This module focuses on what Client Reputation is and how it fits into Akamai's layered defense concept. **LAB: CLIENT REPUTATION**

20	**MODULE 8: MALWARE PROTECTION** This module covers the basics of Malware Protection, including overview, configuration, and troubleshooting
60	**MODULE 9: REPORTING AND ALERTING** This module demonstrates how to identify and utilize the different reports used in analyzing Network Lists, DOS Protections, Rate Controls, Slow POST protection, ASE rules, and Patternbased bots. The Security Dashboard, Security Center, and Web Security Analytics will be highlighted. The module concludes with best practices around setting up notifications within the Security Center. **LAB: SETTING UP WSA ALERTS IN SECURITY CENTER**
90	**MODULE 10: TUNING AND MOVING INTO DENY** This module delves into how and when to set rules for the Adaptive Security Engine within AAP-ASM into Deny mode. **LAB: TUNING WEB APPLICATION FIREWALL**
30	**MODULE 11: DEVOPS + SECURITY (DEVSECOPS)** This module explores in detail the use of DevSecOps philosophies to automate security tasks using APIs as well as the security functionality available via Akamai APIs. This module also explores configuring reporting options for the SIEM integrations. **LAB: USING THE APPSEC API**
30	**MODULE 12: SUMMARY** **LAB: TESTING YOUR CHANGES**
60	**Survey, Quiz & Certification**