AKAMAI FRAUD MANAGEMENT

Course Overview and Agenda

March 2023

Course Overview

The Akamai Fraud Management course covers the current threat landscape, attacker motivations, and technical mitigation strategies for automated non-human (bot) attacks. These range from a single host running command-line scripts to distributed botnets actively trying to appear as legitimate clients. Attack types covered range from basic page/price scraping to more advanced credential stuffing attacks.

The participants learn how our fraud management products detect and mitigate unwanted bots using AI models for user behavior analysis and browser fingerprinting. The course demonstrates Akamai's Bot Manager Premier (BMP) product - how it can collect and evaluate different signals (network characteristics, device characteristics, and human interaction data) to determine if a browser session is run by a human or an automated machine. The course covers the new Bot Score detection engine and how it helps manage False Positive/False Negative response balance, and the new Account Protector product which mitigates the most complex credential stuffing attacks. In addition to common mitigation strategies such as deny, tarpit and slow, students will also learn and implement advanced mitigation techniques available such as conditional actions, CAPTCHA and crypto challenges in hands-on lab environments.

Objectives

After completing this course, participants will be able to do the following:

- Describe the basics of the Akamai Intelligent Platform.
- Provide an overview of the Akamai Cloud Security Solutions portfolio.
- Identify the top bot use cases Akamai customers encounter.
- Explain how to mitigate various types of bot attacks using Bot Manager.

- Configure Bot Manager actions appropriate for each use case.
- Using Akamai Control Center, prepare and deploy a Bot Manager configuration
- to mitigate bot attacks and view detailed reporting on bot activity.
- Describe how to tune and troubleshoot basic bot false positive and false negative issues to improve your security posture.
- Identify the use case for Account Protector and describe its key features.
- Configure Account Protector to mitigate account takeover.

Prerequisites

To maximize your time in the class and ensure you get the most out of the three-day training, Akamai University recommends that you will have completed the following prerequisites:

- You have at least one Akamai Security Product on contract
- You have an account set up in the Akamai Control Center (control.akamai.com)
- You have deployed an Akamai Configuration to staging or production

Agenda

The Akamai Fraud Management course curriculum can be delivered either as:

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

The agenda for this training is listed below.

Duration (min)	Module Name & Description
60	**MODULE 1: INTRODUCTION** This module is an introduction to Akamai's Cloud Security Solutions portfolio, and a reference architecture for Bot Manager discussion
60	**MODULE 2: THREAT LANDSCAPE: THE BOT PROBLEM** This module is a discussion on the various pain points that bots cause. In this module we examine why defense is difficult, as well as the top five bot use cases that Akamai customers encounter. This module also reviews how attackers set up both a simple single host bot as well as a complex Command & Control botnet. The various types of methods and frameworks for creating a botnet are discussed to create a full understanding of the bot problems organizations face today.
75	**MODULE 3: REFERENCE ARCHITECTURE** This module is a technical review of Akamai's Security Cloud Security Solutions portfolio and discusses how the products work together in defense of customer web sites for bot mitigation. **LAB: CREATING A DELIVERY CONFIGURATION / SETTING UP A SECURITY CONFIGURATION** These labs will introduce the learner to Akamai Control Center and will facilitate the learner in setting up a basic property using Property Manager. The learner will then create and activate a basic security configuration using Bot Manager.
75	**MODULE 4: BOT MITIGATION** This module will identify mitigation strategies available in Bot Manager and review appropriate mitigation strategies based on the type of botnet detected. **LAB: CONFIGURING PASSIVE AND ACTIVE BOT DETECTIONS** In this lab the learner will analyze the bot traffic targeting a site and configure the Passive and Active bot detection methods to mitigate basic bot traffic. The learner will also configure the Conditional and Serve Alternate response actions in order to mitigate bots.
60	**MODULE 5: MANAGING PATTERN-BASED BOTS** This module introduces the key features of our Bot Management products, including Bot Visibility and Mitigation and Bot Manager Standard, and how to use Akamai Bot Categories and Custom Bot Categories. Basic Bot Detections such as Request Anomaly, User-Agent, and Validation are discussed.

45	**MODULE 6: MANAGING MORE COMPLEX BOTS** This module introduces Bot Manager Premier and BMP SDK. The technical approach to Behavior Anomaly Detection, API Definition and Resource Purpose, and the new Bot Score model is discussed. This module also covers the Bot Manager Premier Mobile solution and Software Development Kit (SDK) available for mobile apps protection. **LAB: CONFIGURE BEHAVIOR ANOMALY DETECTION (BOT MANAGER PREMIER)** In this lab, the learner will create an API definition to define the login endpoint as an API resource, configure Behavioral Anomaly detection in Monitor mode, and test the capability. The learner will also configure and implement Challenge actions to prevent requests that might have some bot characteristics from being directly denied.
60	**MODULE 7: ACCOUNT PROTECTOR** This module introduces the new Fraud management solution known as Account Protector, and discusses the account takeover (ATO) problem, how Account Protector assists with ATO types of attacks, and how to configure Account Protector. **LAB: CONFIGURE ACCOUNT PROTECTOR** During the course of this lab, the learner will update the the API definition for the login endpoint in Akamai Control Center (ACC) to add origin response and success conditions, configure Account Protector for the endpoint in Monitor mode and verify that Account Protector is working via Web Security Analytics (WSA).
30	**MODULE 8: MSS BMP** This module will review the value proposition features of Managed Security Services and describe the key features of MSS for Bot Manager Premier.
60	**MODULE 9: REPORTING + ALERTING** This module will assist the learner in Identifying and using various reports and tools available in Security Center for analyzing Bot traffic and setting up notifications. Tuning Bot Manager based on your analysis will be discussed as an introduction to the subsequent module.
60	**MODULE 10: TUNING AND TROUBLESHOOTING** In this penultimate module, based on their knowledge of Security Center learners will learn how to tune bot definitions and set them into Deny Mode. The module will also review basic troubleshooting steps for Bot Management and Account Protector and review basic escalation steps for Bot Management.
15	**MODULE 11: SUMMARY** This final module provides key takeaways for the entire course and provides a final opportunity for learners to complete lab work, receive job aids and other materials, and a class discussion on followup questions or concerns.
60	**Survey, Quiz & Certification**