AKAMAI ZERO TRUST SOLUTIONS

Course Overview and Agenda

March 2023

Course Overview

The Akamai Zero Trust Solutions course will cover the Zero Trust architecture and Akamai's enterprise products including Secure Internet Access Enterprise (SIA) and Enterprise Application Access (EAA). The participants will also learn about Akamai Multi-Factor Authentication.

Objectives

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

- Provide an overview of the Akamai Zero Trust model.
- Provide an overview of the Akamai Enterprise Solutions portfolio.
- Identify the top use cases Akamai customers encounter when protecting their domains from threats and malware.
- Describe in technical detail the features and benefits of the Akamai Secure Internet Access Enterprise (SIA), Enterprise Application Access (EAA), and Akamai MFA.
- Configure SIA and Akamai MFA in Akamai Control Center.
- Identify the top use cases Akamai customers encounter when creating authentication policies for applications in their environment.
- Describe various authentication mechanisms available to applications.
- Configure EAA for various authentication use cases using ACC.

Agenda

The Akamai Zero Trust Solutions 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
75	**MODULE 1: ZERO TRUST OVERVIEW** This module introduces the need in the industry for a zero-trust model, provides an introduction to Akamai's Zero Trust and Enterprise Solutions portfolio, and presents a reference architecture for use in the course.
150	**MODULE 2: ENTERPRISE THREAT PROTECTOR** This module will provide a technical review and a deep dive into Akamai's Enterprise Threat Protector (ETP) product and discusses how the ETP product functions. **LAB: ETP** This module features an instructor-led demo and student lab where the instructor will demonstrate configuration of a simple ETP policy before having the student create and deploy an ETP policy.
120	**MODULE 3: ENTERPRISE APPLICATION ACCESS OVERVIEW** This module is a presentation on the need for Enterprise Application Access in today's complex application environment. This will cover the changing landscape of cloud and legacy applications, networks, user communities and authentication methods which present challenge in application security.
165	**MODULE 4: EAA DEEP DIVE 1** This module will review the EAA product in depth, covering the setup of EAA connectors for various authentication mechanisms and applications as well as the EAA client connector. **LAB: EAA** This hands-on instructor-led lab will serve as a capstone assignment. In this lab, students will configure various application access types in ACC, as well as set up the Client Connector.
45	**MODULE 5: EAA DEEP DIVE 2** This module will review the EAA product in depth, covering the setup of EAA connectors for various authentication mechanisms and applications as well as the EAA client connector.
90	**MODULE 6: AKAMAI MULTI-FACTOR AUTHENTICATION** This module presents the Akamai Multi-Factor Authentication solution. **LAB: MFA** The Akamai MFA lab utilizes the EAA lab infrastructure and builds upon the existing EAA configuration. In the lab, students will enable multi-factor authentication for a web application by integrating the EAA identity provider with Akamai MFA.
60	**SUMMARY / SURVEY/ QUIZ AND COURSE CERTIFICATION**