radware

Cloud WAAP – Advanced

Training Course Outline

1 Introduction

The landscape of web application development is evolving rapidly, with increasing complexity and accelerated release cycles driven by DevOps practices. As organizations prioritize delivering high availability and seamless user experiences, web applications are not only more critical but also more susceptible to a range of security threats, including data breaches and financial losses. In addition to traditional vulnerabilities, the proliferation of APIs and automated traffic—such as bots and large-scale WebDDoS attacks—further amplifies the risk profile for modern enterprises.

Radware's Cloud WAAP Service provides enterprise-grade protection for web applications, APIs, and services. It includes advanced API security, integrated Web DDoS defense, Bot Manager, LLM Firewall, and Agentic AI protection, all managed through centralized Security Policies for consistent and scalable security.

2 Purpose and Scope

This course, **Cloud WAAP Advanced**, is a structured 2-day training course.

It consists of a practical and a theoretical part.

This training program commences with a comprehensive overview of Security Policies, providing participants with a thorough understanding of their purpose and configuration within the Cloud WAAP environment. Additionally, the course addresses advanced strategies for defending against Web DDoS attacks, outlining mitigation techniques and best practices. Finally, participants will explore methods for identifying and preventing bot attacks, including the utilization of specialized tools and features designed to detect and manage automated threats. This structured approach ensures attendees acquire both theoretical knowledge and practical skills necessary for robust web application security management.

3 Target Audience and Prerequisites

This training program is intended for technical professionals who possess a strong foundational understanding of application technologies and have successfully completed Level 1 training. It is specifically tailored for individuals seeking to further deepen their expertise in the Radware Cloud WAAP solution, enabling them to acquire advanced knowledge and practical skills necessary for implementing, configuring, and managing comprehensive web application security within enterprise environments.

4 Objectives

- Understand how to use Security Policies to manage Cloud WAAP
- Gain an understanding of the primary capabilities of Cloud API protection and their operational mechanisms.
- Install and deploy a Cloud WAAP application to secure an API application
- Develop proficiency in monitoring Cloud API protection functionalities
- Understand how the Bot Manager can be utilized to protect applications from bot attacks
- Understand how the Web DDoS protection works
- Understand how the LLM Firewall works
- Understand how we can protect Agentic AI

5 Presentations and Hands-On Labs

Presentations Day 1:

- Introduction to Radware's Cloud Web Application and API Protection (WAAP) service
- API Background Information
- API Protection
- API Testing
- Business Logic Attack Protection
- Token Authorization Protection

Hands-On Labs Day 1:

- Access the Cloud WAAP portal
- Create your application
- Configure API Protection on the application
- Configure the remote system to access the application
- Run attacks
- Review security events

Presentations Day 2:

- Security Policies and related protections
- Bot Manager
- Web DDoS
- LLM Firewall
- Agentic AI

Hands-On Labs Day 2:

- Configure a security policy and attach it to the application
- Configure and test Bot Protection
- Configure and test Web DDoS
- Configure LLM Firewall protection

North America
Radware Inc.
575 Corporate Drive, Lobby 1
Mahwah, NJ 07430
Tel: +1-888-234-5763

International
Radware Ltd.
22 Raoul Wallenberg St.
Tel Aviv 69710, Israel
Tel: +972 3 766 8666