Connected World.
Connected Experiences.

Tech Mahindra

CASE STUDY

WAF IMPLEMENTATION TO PROVIDE SAFE INTERNET BANKING EXPERIENCE FOR A LEADING INDIAN BANK

BUSINESS CONTEXT

The Client aimed to upgrade their Security Infrastructure to improve cyber safety. They faced the following challenges:

- Provide Safe Internet banking environment to Bank's retail and merchant customers and prevent network and application level attacks information
- Offer protection against risks arising from DDOS and Web Attacks
- Close VA observations and Maintain configuration as per Security Configuration Document
- DR Drills and Migrations

Copyright © 2021 Tech Mahindra. All rights reserved.

APPROACH AND SOLUTION

Tech Mahindra catered to the client problem as follows:

- Implemented Internet facing DDoS common to all segments that provides Behavioral and Volumetric DDoS protection
- Implemented SSL Off-loader to inspect offending DDoS traffic
- Implemented Barracuda WAF across all the segments in inline monitoring mode that offers protection against OWASP top 10 and other generic web attacks
- Maintain SCD, VA Closures and Security Trackers
- Security Incident Handling

IMPACT & HIGHLIGHTS

Reduced WAF log size by fine-tuning to accommodate the application environment by reducing false positives

Integration of WAF with Bank's SOC. Security incident handling and analysis for SOC reported events

Integration of WAFs with Bank's PIMS solution

ESRM.Communications@TechMahindra.com

Tech Mahindra
Connected World. Connected Experiences.

Copyright © Tech Mahindra 2021. All Rights Reserved.
Disclaimer. Brand names, logos and trademarks used herein remain the property of their respective owners.