

SERVICE DESCRIPTION

ModSecurity Commercial Rule Set

Overview

Trustwave's ModSecurity Commercial Rule Set ("**Service**") provides Client custom rules for the open-source web application firewall (WAF) ModSecurity. The following description sets out the parameters of the Service, as may be further modified by an applicable SOW or Order Confirmation between Trustwave and Client.

Service Features

ModSecurity assists in providing protection against known attacks that target vulnerabilities in software and applications. However, to effectively provide such protection, ModSecurity must be configured with rules that help it recognize threats and defend against them. Trustwave provides this Service for ModSecurity version 2.x.

The Service includes the following features:

Rule Set Generation and Maintenance

The Service complements the Open Web Application Security Project (OWASP) ModSecurity Core Rule Set (CRS) by enhancing the basic payload protection offered by CRS. CRS does not correlate specific attack vector locations (such as URL and parameters) with publicly disclosed vulnerabilities. The Service provides Client with a set of rules that establish custom virtual patches for various public vulnerabilities.

Trustwave may collect data from numerous sources to generate a commercial rule set. This set will automatically be updated daily and as otherwise needed. Sources include:

- Public vulnerability data such as the Open Source Vulnerability Database (OSVDB)
- Honeypot systems such as the WASC Distributed Web Honeypot Project (<http://projects.webappsec.org/Distributed-Web-Honeypots>)
- Trustwave WAF client data Analysis

The Client acknowledges that

- The Service does not include ModSecurity WAF support; and
- The Service does not include implementation support.

Client Obligations

For Trustwave to provide this feature of the Service, Client will

- Update and maintain ModSecurity on its system; and

- Determine the configuration and suitability of its security solutions, including where Client obtains advice and consultancy from Trustwave.

Trustwave Obligations

For this Feature, Trustwave will

- Research threats to generate new rules and to maintain the Service.

Additional Information

Client may purchase ModSecurity implementation support as an add-on service, which assists Client with the Service configuration including assistance with false-positives, false-negatives, and other support issues.

Definitions

All capitalized terms not defined in this document have the meanings ascribed to them in Trustwave's Master Terms and Conditions available at <https://www.trustwave.com/en-us/legal-documents/contract-documents/> or in the applicable Statement of Work or Order Confirmation between Trustwave and Client.