Addendum to Security Technology Management Service Description

Cloud Web Application Firewall (WAF)

Scope, Features and Responsibilities

Trustwave's Security Technology Management for Cloud WAF (the "WAF Service") monitors and helps protect your web application(s) from attack. Trustwave's security engineers will monitor security events from Client's web application(s)'s HTTP/HTTPS requests and responds 24x7x365 to identify evidence of suspicious activity or application integrity issues, filter out false positives, and notify Client of suspected Security Incidents.

- The WAF Service will follow and incorporate the Security Technology Management Service Description unless otherwise specified.
- Client will have read-only access to the Akamai Control Centre in order to manage the WAF Service.
- The Service Level Agreement ("SLA") specifically for the WAF Service ("WAF SLA") shall solely apply to the WAF Service.
- Integration to core detection capabilities is provided by the Managed Security Threat Monitoring Service.

Service Features

- Basic Service Features
    - Change Management
    - Security Incident Management
- Optional Service Features
    - Security Policy Review and Optimization Analysis
    - Client Success – Named Security Advocate

Basic Service Features

Change Management

The WAF Service will adopt the following definition of Change Management.

Change Type	Definition
Emergency	Unplanned changes to the policy configuration or platform settings based on approved requirements from the Client. Changes that: • Cannot be planned in advance

	• Are required for the restoration of a main function of the website, thus requiring prompt actions E.g. • Urgent changes requested on non-working day • Urgent changes requested due to changes in origin component
Standard	Planned changes to the policy configuration or platform settings based on approved requirements from customer. Changes that: • Can be planned in advance • Are required as part of on-going platform improvements E.g. • Planned implementation of threat review recommendations for improvement of security posture

Transitioning Services

Transitioning services are available for the WAF Service and are described further in the "MSS Transition Service Description. Addendum to MSS Transition Service Description- Managed Cloud WAF".

Managed Security Threat Monitoring and Security Incident Management

Managed Security Threat Monitoring

Managed Security Threat Monitoring and Security Incident Management includes 24 x 7 x 365 monitoring and investigation of security events originating from the Managed Cloud WAF, and determination of level of risk and appropriate escalation of a security event. Trustwave applies automated analytics to the security events collected from the Managed Cloud WAF and a Priority rating in accordance with the below table is allocated to each escalated security event based on the threat intelligence within the technology analytics engine.

A Priority rating of 1 or 2 is identified as a Security Incident, and each Security Incident is analyzed and further investigated to identify false positives and escalate to Client in the case of a true security event based on the SLA defined for the respective Priority ratings.

Priority	Definition
P1	Confirmed ongoing true-positive attack with visible impact on a protected digital property
P2	Confirmed past true-positive attacks with visible impact on a protected digital property Suspected ongoing attacks on a protected digital property
P3	Suspected past attacks on a protected digital property Attacks that are already blocked at DMS (thus, no impact to origin resources) Proactive heightened security monitoring on a potential future attack
P4	Any other security escalations that do not fall within P1, P2 or P3.

Security Incident Management

Security Incident Management activities consist of:

- Documentation of all available information on the incident, including nature of the incident, but not limited to the properties that appear to be affected, source(s) of the incident, when the incident first appeared to begin.
- Notification and update communication to the nominated Client contact in accordance with the escalation process and as determined by the Priority rating of the relevant Security Incident.
- Response to notification of a Security Incident identified by Client.
- Security Incident investigation.
- Mitigation strategy recommendations.
- Implementation of Client approved threat mitigation procedures.
- Confirmation of implementation status.
- Event logs monitoring to determine if an identified attack has been mitigated.
- Document incident, observations, recommend policy changes based on each Security Incident.

Trustwave Responsibilities and Acknowledgements

- Review security events originating from the Managed Cloud WAF and help identify potential Security Incidents.
- Investigate and analyze Security Alerts to identify false positives and notify Client in the case of a suspected actual or potential threat.
- Help identify and prioritize Security Incidents and escalate to designated point-of-contacts based on the priority of the incident and appropriate response.
- Create an exception rule or turn off the relevant rule for identified false positives.
- Update status of Security Alerts and Security Incidents and record all related communication in the ticketing system.
- Make available to Client a detailed summary of an individual Security Incident, issued on closure of the relevant Security Incident ticket.

Client Responsibilities and Acknowledgements

- Nominate and update authorized escalation point-of-contact for potential Security Incidents.
- Validate the prioritization of a Security Alert according to its business impact and notify Trustwave of Priority rating classification errors.
- Work with Trustwave to investigate, mitigate and/or remediate and resolve each Security Alert and Security Incident, by providing relevant personnel and ensuring support and engagement of third parties as required.

- Provide Trustwave with requested information and confirmations in a timely manner.
- Maintain system access to confirm updated status and/or resolution of Security Alerts and Security Incidents.
- Coordinate with Trustwave regarding appropriate actions needed to implement any Client environment configuration.
- Maintain access to the platform to confirm updated status and/or resolution of Security Alerts and Security Incidents.
- Access the platform to receive notifications, view, download and track the status of and respond to Security Alerts and Security Incidents.
- Request changes in accordance with the Trustwave Change Management policy documented in the Security Technology Management Service Description.

Optional Features (Additional Fee)

Security Policy Review and Optimization Analysis

Periodically reviewing the security policy configuration is necessary to ensure that the WAF is sufficiently protecting the web application from new vulnerabilities that could be exposed due to changes in Client's environment. Security Policy Review and Optimization Analysis is performed independently for each WAF policy and includes a statistical analysis of Security Alerts relating to Client's relevant web application policy to evaluate the rules triggered (false positives & true positives) and recommend related configuration optimization.

Upon approval from Client regarding the recommended configuration optimization, Clients may request that any recommended changes be implemented via the Change Management process. The recommended configuration will include the estimated time and effort needed to fulfill the request. Clients who are entitled to Professional Services Hours may choose to draw down and utilize the allocated hours where sufficient.

Trustwave Responsibilities and Acknowledgements

The SOC will respond to Security Policy Review and Optimization Analysis requests made within two business days of receipt and will include in that response an estimated time to fulfill the request and an estimate of the number of hours to fulfil the request, or alternatively, with follow-up questions to clarify the request.

Perform Change Management activities when requested and in compliance with Trustwave policies.

The SOC will provide emergency security configuration assistance in response to confirmed attacks.

Client Responsibilities and Acknowledgements

Request that any change request be implemented per the guidelines under Change Management activities.

Client Success – Information Security Specialist (ISS)

ISS are security trained professionals who provide a point of contact between the Client and Trustwave for in-scope products and services. ISS assist with implementation and management of security activities, process, and policies. ISS act as technology expert for Managed Cloud WAF and are the ones who understand the Client's business needs and Akamai security configuration.

ISS provide analysis and recommendations based on Client's specific needs in consultation with the SOC team. They assist with onboarding, ongoing maintenance, and consultation for the WAF Service. Please note however, that solely the SOC serves as the 24x7x365 contact center for Client, and that the ISS is a senior level security advisor and operational relationship manager that is not available 24x7x365.

Definitions

Security Alert means one or more Security Events of certain significance which have been escalated as a Security Alert, where the application of automated threat analysis correlation rules of certain attributes have identified the Security Event as being a security threat and requiring further analysis, attention and investigation. Security Alerts are evaluated through an incident management process where they are categorized and appropriate actions are taken based on the level of severity.

Security Event means an event or series of events, relating to a potential security threat.

Security Incident means a Security Alert of certain significance, which having been analyzed and investigated by the GTO team is, identified as a security threat and escalated to the Client based on the severity assigned by a threat analyst.