SERVICE DESCRIPTION

Managed Intrusion Detection Security

Service Description Overview

Trustwave's Managed Intrusion Detection Security (IDS) service helps the Client monitor for evidence of malicious network or application attacks. Trustwave's 24x7x365 network security engineers will manage the supported Client IDS device(s), analyze events and recommend to the Client appropriate steps to take in the case of a suspected threat. Trustwave will monitor the events on the Managed IDS Device(s) to help identify evidence of suspicious activity and filter out false positives. Through Trustwave's TrustKeeper Client Portal, the Client has 24x7 online access to suspect activity event logs and reporting. The availability of a record of attack events and subsequent analysis assists the Client in meeting its internal control and compliance requirements.

The Managed IDS service consists of:

Service Provisioning – the performance of remote activities required to establish the service within a steady state. Provisioning connects the Managed IDS Device(s) to the Trustwave Platform and the features and functionality of IDS Service system management and security threat analysis. The IDS Service includes the collection and assessment of the Client Initiation Information and the initial configuration of the Managed IDS Device(s).

System Management – the ongoing configuration of the Managed IDS Device(s), policies, rulesets, the management, maintenance, health monitoring and the implementation of Security Updates and Product Updates to, the Managed IDS Device(s). The Trustwave Security Operations Center (SOC) teams provide these services through globally located facilities.

Security Threat Analysis – monitoring and investigation activities by the Global Threat Operations (GTO) team through globally located facilities. These activities include the monitoring, analysis, correlation and synthesis of security information provided by the monitored Managed IDS Device(s) as well as the application of threat intelligence from the Trustwave Spider Labs malware research teams and threat database.

Base Features of Service

Basic service features overview

- The Managed IDS Service includes the following basic service features; Review, scoping of the Client's IDS system, Initial baselining and tuning of the Managed IDS System Device(s), policies and rulesets;
- 24x7 security event monitoring and investigation;
- Detection engine Security Updates and Product Updates; and the management, maintenance and provision of technical support assistance, for supported IDS System Device(s) and features.
- TrustKeeper Client Portal providing access to Tracking of provisioning progress;
- 24x7 Security Event and Security Alert reporting;
- Change and support requests creation and management; track status of Provisioning and Implementation

Provisioning and Implementation

Implementation and Delivery

- The provisioning team is the Client's first point of interaction with Trustwave after the contract is executed. This team is responsible for working with Client to review and analyze the Client Initiation Information and provision, implement the Managed IDS Device(s) into the Client's production environment so that the services can be handed over to the SOC for on-going management, maintenance and support. Please see the Trustwave Provisioning Guide for additional details on the service implementation.
- The Managed IDS service is deemed to be delivered and operational when the SOC has management control of the Managed IDS Device(s); the SOC is able to view the Managed IDS Device(s); and the Client has access to the TrustKeeper Client Portal to view event data and reports.

Device and environment assessment

- Trustwave provisioning engineers work with the Client to help ensure optimal service configuration, including assessment of the completeness of the Client Initiation Information provided;
- IDS policies and IDS rulesets; and placement and configuration of the Managed IDS System Device(s).
- Assessment of the configuration of the Managed IDS Device(s) to determine if current version and features are consistent with Trustwave supported device requirements.

Device configuration

- Trustwave provisioning will work with the Client to verify that the Managed IDS System Device(s) are integrated into the Trustwave Platform, in a "supported state", confirming any Product Updates required to the Managed IDS System Device(s) required to meet Trustwave's supported device requirements;
- that the Managed IDS System Device(s) communicate with Trustwave Platform for log data collection, device management and control;
- an active secure connection between the Trustwave Platform and the Managed IDS System Device(s);
- Client has completed a comprehensive test plan to review all impacted Client systems associated with the Managed IDS System Device(s) and/or Managed IDS service.

Device baselining

- GTO analysts monitor, review and work with the Client to tune and update the configured security policies, in the Managed IDS Device(s) to an approved state for Trustwave standard operations
- Once baseline policy is configured, that policy will be monitored and recommendations made for tuning. Once the configuration is optimized, the baselining period ends and the Managed IDS Device(s) are prepared for transitioned to Trustwave standard SOC operations, for monitoring and management.

Trustwave Managed Security Portal

- The Trustwave Managed Security portal provides clients with access to the expertise of the SOC staff and the security information and analysis provided by the supporting Trustwave managed services infrastructure.
- The Trustwave Portal provides a method for the Client to Securely communicate with Trustwave MSS Provisioning and SOC Personnel to upload documentation and security policies and and includes Designated client contact information.
- Allows client to review current security events and Security Alerts of Client's Trustwave-monitored service, as well as historical data;
- Create and track Change tickets and support.

Trustwave Responsibilities

- Establish and maintain contact with the Client and navigate the Client through the provisioning process until the Managed IDS System Device(s) are handed over to SOC for on-going management, maintenance and support;
- Initiate provisioning activities with Client and collect, review and assess the necessary information relating to the Managed IDS System Device(s) and operating environment as necessary to complete the provisioning process;
- Assess, configure and baseline the Managed IDS System Device(s) based on information and instructions provided by Client;
- The Managed IDS System Device(s) are functioning according to the service delivery design; and Managed IDS System Device(s) and the management and security event collection are active within the Trustwave Platform.

Client Responsibilities

- Make available an onsite resource capable of installation and troubleshooting of the Managed IDS System Device(s) and Client environment;
- Provide remote access to on premise infrastructure to accommodate installation and configuration of any Managed IDS System Device(s);
- Provide appropriate credentialed access to Trustwave, to the Managed IDS System Device(s);
- Provide and maintain a secure connection between the Managed IDS System Device(s) and the Trustwave Platform, which is compatible with available Trustwave connection standards;
- Client must develop and complete a comprehensive test plan to review all impacted customer systems associated with the provisioned Managed IDS System Devices prior to commencement of the Device Baselining activities
- Read and confirm the Client understands all provided user guides and documentation; Participate in and confirm the Client's understanding of the processes explained during the Welcome call;
- Client must acquire and maintain valid licenses and maintenance contracts for Managed IDS System Device(s); and
- Client acknowledges that Trustwave provisioning, management and threat analysis services are performed remotely. Any on-site provisioning or support services required by the Client, would be acquired separately as a Trustwave consulting service, and Trustwave is not responsible for delays in provisioning due to delays or inaccurate Client Initiation Information.

System Management

- The Managed IDS service includes the configuration, health monitoring and provision of Product Updates to the Managed IDS Device(s). These management features ensure that the Managed IDS Device(s) are performing their function within the Client environment as designed.
- The Trustwave SOC manages the Managed IDS Device(s) to ensure that the Managed IDS Device(s) are active; Track the version of firmware or software that is active on the Managed IDS Device(s); Apply Product Updates and Security Updates to the Managed IDS Device(s).

Health status monitoring

- The health status-monitoring feature of the Managed IDS Service monitors the network availability of the Managed IDS Device(s) to ensure they are visible to the Trustwave Platform.
- The Managed IDS Device(s) are monitored to help detect when these devices are no longer showing as active within the Trustwave Platform. This includes Initial steps taken to assess the cause of the offline status of the relevant device and remediate the issue if possible; The SOC analysts will contact the Client's technical contact or other designated contact to notify the Client if remediation steps available to Trustwave

are not successful;

- The notifications sent to the Client regarding the device status will be provided within the time requirements specified in the SLA. The SOC analyst will activate an RMA Process and provide remote assistance, support and configuration, in respect of any repaired or replaced Managed IDS Device(s).

Product and Security Updates

- The Trustwave SOC will monitor the availability of Product Updates and Security Updates and apply those updates to the Managed IDS Device(s). When a Product Update or Security Updates becomes available, a Ticket will be created and assigned to the Client by the Trustwave SOC;
- Product Updates and Security Updates available will be scheduled with the Client for implementation; While the Trustwave SOC will give consideration to accommodate the Client's preferred maintenance window and apply any threat protection features with the least disruption to the Managed IDS Device(s), as possible. The Trustwave SOC will implement the relevant Product Updates and Security Updates within timeframe required depending on priority, to ensure that the Managed IDS Device(s) are operating, and the Managed IDS Service is provided, as designed.
- All Security Updates and Product Updates for Managed IDS Device(s) software and underlining Managed IDS Device OS will be completed during version upgrades. Bug fixes will be applied as Product Updates to the Managed IDS Device(s) only when applicable to that device.

Trustwave Responsibilities

- Maintain management connection to the Managed IDS Device(s). Monitor the Managed IDS Device(s) to ensure their active online status and that they are available.
- Notify Client within SLA timeframe if management connection is unavailable and cannot be restored by Trustwave.
- Identify available Product Updates and provide remote assistance, support and configuration, in respect of any repaired or replaced Managed IDS Device(s). Apply Security Updates, Product Updates as they are made available within timeframe required depending on the relevant update's priority.
- Create a Managed IDS Service Ticket and schedule the Product Update, Security Update or rule update with the Client.
- Attempt to resolve any connectivity or system issues identified in order to return the device to a steady state of operation.

Client Responsibilities

- Inform Trustwave of all Client environment maintenance activity and changes that may impact on Trustwave's ability to provide the Managed IDS Service, as designed.
- Access the TrustKeeper Client Portal, respond to Tickets and confirm scheduled implementation of Product Updates and Security Updates.
- When requested by Trustwave, provide onsite support, for the Managed IDS Device(s), to resolve connectivity or support issues.
- In relation to the RMA Process; Confirm delivery of an RMA Device. Perform the physical installation of an RMA Device.
- Contact the SOC to arrange for Trustwave remote support and configuration of an RMA Device.
- The Client acknowledges that implementation of necessary Product Updates and Security Update is not an optional feature of the Managed IDS Service.
- Failure to implement a required Product Update, Security Update or rule update as required, may adversely impact the operation and functionality of the Managed IDS Device(s).

Security Threat Analysis and Investigation

- Security Threat Analysis and Investigation includes the monitoring and investigation of the security information provided by the Managed IDS Device; and the determination of level of risk and appropriate response to a given security event.
- The Managed IDS Device will help identify network activity related to malware or suspicious activity. The combined intelligence gained from the correlation and analysis of all available security related Managed IDS Device data assists the GTO team to help identify and respond to suspected Security Incidents.

Automated Threat Analysis

- Trustwave's proprietary threat analysis engine considers aggregated Trustwave client security and infrastructure information, to help identify potential indicators of security attacks and attempts to compromise a Client's network environment.
- Automated analytics are applied to the Security Events collected from the IDS Management Console or the Trustwave Platform (depending on the deployment model selected). Based on threat intelligence within the Trustwave analytics engine, a level of importance is allocated to each Security Event.
- Security Events that have been escalated by the automated threat analysis engine, are identified as a Security Alert and reported on independently within the TrustKeeper Client Portal and stored for further event investigation activities by the GTO team.

Investigation and Incident Identification

- For a consistent methodology of investigation across the globally distributed GTO teams, this process includes the advice and guidance from Trustwave Spider Labs malware research, threat intelligence and incident response teams. The GTO team will evaluate the available information it has to the point of helping to identify potential attack attempts or Security Incidents. Where the investigation identifies a Security Incident, the GTO team will notify the Client of the results. Where the investigation does not result in a Security Incident, the GTO team will record the investigation without Client notification. The Client may access the history of investigations performed by the GTO via the TrustKeeper Client Portal.
- Security Alerts are analyzed by the GTO team on a 24 / 7 / 365 basis
- GTO analysts leverage all available Client information and intelligence associated with the Security Alert to determine severity of the alert.
- Where warranted, the GTO analyst will escalate a Security Alert being investigated, to a Security Incident and assign it a priority based on the criteria specified. The priority level defines the response actions to be taken by the GTO and the Client.
- The GTO analyst categorizes the Security Incident based on the descriptions outlined for the IDS Service.

Trustwave Responsibilities

- Review security events collected by the Managed IDS Device(s) and helping to identify potential Security Alerts. Investigate and analyze Security Alerts, help identify false positives and notify Client in the case of a suspected actual or potential threat.
- Help identify and prioritize Security Incidents and notify designated Client personnel based on the priority of the incident and the appropriate response.
- Classify Security Incidents according to the categories defined.
- If needed, escalate the Incident based on its priority and according to the service level agreement ("SLA").
- Create an exception rule or turn off the relevant rule, for identified false positives;
- Maintain updated status of Security Incidents on the TrustKeeper Client Portal. Record all communications in the Ticketing system.

Client Responsibilities

- Validate the prioritization of a Security Incident according to its business impact and notify Trustwave of priority classification errors.
- Work with Trustwave to resolve each 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 access to the Client TrustKeeper Portal to confirm updated status of Security Incidents.
- Request changes in accordance with the Trustwave change management process, and use and access the TrustKeeper Client Portal to log tickets, receive notifications, view, download and track the status of and respond to, Security Alerts and Security Incidents.

Reporting

- The Managed IDS service includes the following available reporting features through the TrustKeeper Client Portal:
- 7 days of Security Events available in the security activity area of the TrustKeeper Client Portal.
- 110 days of Security Alerts available in the security activity area of the TrustKeeper Client Portal.
- Upon Client request, 12 months of Log Data in csv format, which can accessed securely through the TrustKeeper Client Portal.

Trustwave Responsibilities

- Generate Security Alert and Security Incident reports, and make them accessible through the TrustKeeper Client Portal.

Client Responsibilities

- View available reports through the TrustKeeper Client Portal.
- The Client acknowledges that the available report formats may change from time to time.

Change Management

- Trustwave maintains an overall change control and configuration management procedure for its support infrastructure and associated managed services. Changes that could affect the operation of Client systems are coordinated with appropriate Client IT staff. Trustwave establishes an email address for each Client contact that is used to support communication with the Client and its service contractors responsible for administration of its networks.
- The SOC will assesses and implements change requests submitted by the Client or SOC through the TrustKeeper Client Portal. All requests are evaluated to help ensure that they are aligned with the features included with the service and will not detrimentally impact the security of the Client environment. Typical change request for the Managed IDS Service are Configuration changes to the Managed IDS Device(s) as requested by authorized Client contact or a GTO analyst in response to a known threat and Change reversals as requested by an authorized Client contact.

Trustwave Responsibilities

- Allow authorized Client personnel to submit Security Incidents through the TrustKeeper Client Portal, as needed. Perform change management activities when requested and in compliance with Trustwave policies.
- Validate that the request was submitted by an authorized Client contact, and notify Client if validation is not successful.
- Determine whether the request is in-scope with the terms of the Service.

- Source additional information as necessary to support the implementation of the change request.
- Assess the potential risk that will result from implementation of the change request and advise Client of the outcome. Confirm Client approval to implement the change request after reviewing risk assessment results with Client.
- Confirm Client acceptance of implemented changes. When authorized Client personnel request that Trustwave roll back or reverse a change request Confirm receipt of Client's request for a change reversal. Confirm completion of the change rollback upon successful execution of change reversal activities.
- Execute joint testing with Client to validate the rollback is aligned to Client's request, and gain Client confirmation of the same. Update the change request with information on rollback changes.
- Notify Client a change request is outside the scope of the service and or if additional charges will apply to a change request.

Client Responsibilities

- Submit change requests using the TrustKeeper Client Portal.
- Where the Client does not agree with a Security Incident priority, submit a change management request to change the priority of the relevant Security Incident.
- Provide Trustwave with requested information in a reasonable timeframe and Provide resources to review the risk assessment relating to requested changes. Review, assess and notify Trustwave of approval or non-approval to a proposed change request.
- When required, authorized Client personnel may request that Trustwave roll back or reverse a change request.
    - Submit reversal requests using the TrustKeeper Client Portal, emailing or phoning the Trustwave support team; Provide resources to execute joint testing and confirm the change reversal is aligned with the Client-submitted request and Confirm completion of the change rollback request.

Client acknowledges that change requests that exceed two (2) man days of effort is deemed a project and is subject to acceptance by the Client of separately quoted additional charges.