SERVICE DESCRIPTION

Managed Detection and Response Essential (MDR Essential)

Overview

The Trustwave Managed Detection and Response Essential (MDR Essential) service provides 24x7x365 monitoring of detection and response tools, and provides automated, technology-based detection, analysis and response.

The service leverages the Trustwave Managed Detection service, which monitors system configuration, policies and alerting provided by the Security Operations Center (SOC) teams in Trustwave's global SOC facilities. By adding response and remediation, Trustwave SOC teams provide analysis and response (remediation) activities from global SOC facilities in addition to alerting. Analysts synthesize security information provided by the managed endpoints, other monitored systems within Client environment, and multiple threat intelligence feeds to quickly respond and remediate at the root cause.

Base Features of Service

The MDR Essential service includes the following basic service features:

- Automated technology-based analysis and response
- Root cause analysis, process containment, and remediation
- 24x7x365 Managed Detection monitoring of detection and response tools
- Application of industry-leading cyber threat intelligence for threat detection
- Nine global SOCs and more than 250 security professionals
- Health, status and availability systems management using the Fusion platform

Security Threat Analysis, Investigation and Response (Remediation)

Response

The MDR Essential service is focused on executing the following automated responses to identified security findings:

- Kill a process
- Reverse shell on endpoint
- Download files to endpoint (exe, patch, etc.)
- Upload logs from endpoint
- Quarantine endpoint
- Ban a process

Analysis and investigation process

The MDR Essential service encompasses a two-phase process to provide protection against advanced threats:

- Detection: 24x7x365 analytics with multiple and unique threat intelligence feeds analyze endpoint behavior with a focus on Indicators Of Compromises that may involve memory injections, executables, files changes, and registry modifications.
- Response: On potential signs of compromise, MDR Essential moves to isolate questionable activities to include killing processes and quarantining affected systems.

Execution of analysis, investigation, and response

The SOC team has established incident investigation processes that provide for a consistent methodology of incident response analysis across the global teams.

- The Trustwave SOC Tier 1 (Threat Analysts) provides initial incident analysis (5-7 minutes on average per alert). This first line of escalation provides quick analysis of the incident, primarily leveraging Endpoint Detection and Response (EDR) solution for investigation. Clear threats are remediated when possible. Investigated potential threats are escalated to Tier 2, where a response action is taken, and the finding is closed.

Incident notification protocol

This protocol defines Client's notification preferences (i.e., notification about confirmed incidents only or all suspicious alerts). The Trustwave Managed Security Services (MSS) offerings provide for automated analysis as well as threat analysis performed by SOC analysts. Categories of incident notification are:

- Security alert is raised as suspicious by automated analysis.
- Potential incident is identified by a threat analyst based on initial investigation.
- Incident is believed to exist based of further investigation by threat analyst.
- Threat analyst will implement pre-approved response actions.

Response option	Description
Process blacklisting or hash ban	Implementing a ban on a file hash or updating a process blacklist
Initiate interactive session on endpoint	Enable analysts to open a command shell on the endpoint system
Delete files on endpoint	Removing harmful files on the endpoint systems

Gather files and memory from host	Collection of files and memory from endpoint hosts

Trustwave responsibilities

- Monitor, analyze, and remediate (as necessary according to predefined response guideline) Client's environment as outlined in the MDR Essential service.
- Manage the process in developing a "Client Runbook" that will outline Client priorities and approved response actions that may be executed by Trustwave on Client's behalf.
- Perform change management activities when requested and in compliance with Trustwave policies.
- Allow authorized Client personnel access to the Fusion Client portal to interact with Trustwave personnel and monitor MDR Essential service deployment and execution. The Fusion Client portal will also be used as a repository for Client-approved policies (as defined in Client Runbook) and change management activities.
- Validate that the request was submitted by an authorized Client contact and notify Client if validation is not successful.
- 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.

Client responsibilities

- As defined in this service description, Client will nominate Client personnel authorized to request and or approve configuration and security policy changes and nominate other authorized Client personnel.
- Submit change requests using the Fusion Client portal.
- Provide Trustwave with requested information in a reasonable time as defined by the priority of the request.
- 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.
- Submit reversal requests using the Fusion Client portal, emailing or phoning the Trustwave support team.

Systems Management

Overview

The system management capabilities available provide for management and monitoring of configuration and health status of the managed system. All MSS system management services are delivered from SOCs located strategically across the globe to provide services. The SOC analysts conduct 24x7x365 health and status monitoring and configuration management of the managed systems.

Policy and configuration management

Trustwave maintains an overall change control and configuration management procedure for the managed endpoints; changes that could affect the operation of Client systems are coordinated with appropriate Client contacts (as defined below). Configuration change requests can be made through the following methods:

- Fusion Client Portal – Policy contacts can make policy change requests through the portal specifying all details within the request. These requests are authenticated based on the portal authentication and processed in accordance with the applicable Service Level Agreement (SLA).
- Telephone – Policy contacts can make policy change requests by contacting the SOC and providing the security passphrase previously established.
- Email Request – Policy change requests sent by email must be confirmed as being sent by a policy contact via phone confirmation.

System health and status monitoring

The Trustwave SOC monitors managed systems to ensure that the system is active and its level of performance is within appropriate range. Initial steps will be taken to assess the cause of the performance degradation of the system and remediate the issue, if possible. SOC analysts may need to coordinate with the Technical Contact should additional assistance be required. In the case of on-premise servers supporting the MDR Essential service:

- On-premise servers will be maintained by Client.
- Client retains root access and is responsible for all system-related maintenance.
- The on-premise server will be solely dedicated to the hosted EDR and Next Generation Anti-Virus (NGAV) application (if enabled).
- With the exception of emergency activities, maintenance of the on-premise server will be coordinated with Trustwave Global Threat Operations (GTO) to minimize conflict with the hosted EDR application.
- Customer must provide appropriate non-root access to Trustwave to allow ongoing health monitoring of EDR and NGAV applications hosted on the server.
- Maintaining the security of the management system may include monitoring the security posture through audit log. System monitor activities assist to identify unauthorized access or modifications of the system and to assist with internal control and compliance requirements. Audit logs may be collected to the extent made available by the managed system.

Service Provisioning, Monitoring, and Maintenance

Overview

Service provisioning outlines the activities required to establish the MDR Essential managed service between Trustwave and Client. The execution of service provisioning can be divided into two phases: Client-side implementation and Trustwave SOC onboarding process. Tools are selected and licensed by Client and may be purchased from Trustwave or channel partners. Tools will be configured for read only access by Client, however, data from the technologies can be made available to Client for additional auditing and tracking purposes by request. The Fusion Client portal will be the primary Client interface to track and manage MDR Essential MSS activities. The Fusion Client portal provides access to:

- View current and historical security data and posture information across managed environment (MDR Essential service and other enabled Trustwave MSS activity).
- Communicate securely with Trustwave MSS provisioning and SOC personnel.
- Create and track change requests and other support tickets.
- Update designated Client contact information.
- View service documentation and security policies.
- Create security activity reports.

- Track provisioning progress.

Client-side implementation

The Client-side implementation phase involves the planning and implementation of the technology (known as the EDR or NGAV if selected by Client) and either 1) a hardware or virtual log collection appliance (LCA) or 2) an on-premise Trustwave Security Information and Event Management (SIEM) installation capable of securely passing data to the Trustwave SOC. The goal of this phase is to ensure that Client-side technology is prepared to provide appropriate, consistent Client environment information to the SOC to allow Trustwave to meet service responsibilities and SLAs.

The technology implementation of the tools required to send Client endpoint information into the Trustwave SOC includes the implementation of sensors (light agents) on each endpoint as well as EDR management software (dependent on technology solution) which may be cloud-based or on-premise. Client involvement includes software deployment leveraging Client's current software deployment methodology and may include the implementation of hardware and creation/maintenance of access privileges (dependent on technology solution).

Client may choose to have Trustwave plan and implement their EDR technology and deploy endpoint agents, deploy agents themselves, or hand off to a third party to execute (i.e., vendor implementation). Professional Services may be added to the MDR Essential service to handle execution of Client-side provisioning. In the Trustwave Consulting and Professional Services (CPS) model, Trustwave will be led by the EDR Technology Solutions partner services team; endpoint implementation is not included as part of this service.

If Client has existing security technology management or managed threat detection services, see appendix A.

Trustwave SOC Onboarding Process

Once the Client-side implementation has been completed, the Trustwave provisioning and/or implementation teams (or Technology Solution Partner Professional services team) will work with the Trustwave SOC team to direct the data stream from Client-side EDR solution into the Trustwave SOC. NGAV alerts are not included into this data stream to Fusion platform. NGAV endpoints are handled as a security technology management service and are monitored through the managed detection service. Once Client data is successfully directed into the Trustwave SOC, the SOC team begins an onboarding process in which the data is analyzed and normalized. The onboarding process includes:

- Analyzing the endpoint data individually and collectively to understand the current behavior to the managed endpoints. During this initial step in the onboarding, the SOC team may uncover security threats that need immediate attention as well as "chatty" endpoints that may generate significant amounts of inconsequential/irrelevant data.
- Partnering with Client to understand the expected behavior of each of the endpoints, developing recommendations based on the business significance/priority of the endpoint, and adjusting endpoints accordingly.
- Identifying managed Client contacts
    - Client Contact – Client Contact facilitates the change control process for all managed systems as well as the appropriate notification of security incidents. Fusion Client portal provides levels of access that can be leveraged by Client if needed to delegate levels of access and responsibility within the organization.
    - Policy Contact – The Policy Contact is authorized to make configuration change requests. Policy and configuration changes will not be made on systems unless a Client Policy Contact has authorized the request in writing or directly through a live conversation with an authorized SOC analyst. These contacts are also able to designate other levels of contacts within their organization. The Policy Contact is authorized to:
        - Request and approve configuration and security policy changes.

        - Delegate others within Client organization as Technical or Security Contacts.
    - Technical Contact – The Technical Contact collaborates with SOC analysts to resolve technical issues. The Technical Contact is authorized to:
        - Interact with provisioning and SOC analysts to help ensure system health, accessibility and availability on the network
        - Interact when necessary during system maintenance or other network related maintenance that could disrupt the availability and effectiveness of the system.
        - Submit support requests or respond to Trustwave-initiated support request for the purposes of remediating technical matters.
    - Security Contact – The Security Contact has access to the Fusion Client portal and leverages the security and system-related information provided. In some organizations, security contacts may be assigned security incidents by the Trustwave SOC teams. The Security Contact is authorized to:
        - Request Fusion Client portal support assistance from the SOC.
        - Assign and interact with security incidents within the Fusion Client portal.
        - Request configuration changes because of a security investigation (changes must be approved by a Policy Contact and the change request details stored in the Fusion Client portal).
        - Establish the incident investigation and response protocol. An incident investigation and response protocol will be developed to outline appropriate parameters during an incident addressing both Trustwave and Client activities:
            - Client-side incident response activities may be defined.
            - In the event that some activities may require collaboration with Client resources (such as Client-based IT technical support), Client support protocol procedures will be defined.
            - Protocol steps will include notification, containment, and action to mitigate the active malware and referral to forensic investigation.
            - Some of these protocols may include disabling network interfaces, isolating or terminate processes, shutting down systems, or removing the endpoint from the domain.
            - Specific incident notification and response guidance is provided within this service description under the heading “Security Threat Analysis and Response (Remediation)”.

Trustwave responsibilities

- Navigate Client through the provisioning process until the SOC has ongoing management control of the MDR Essential environment.
- Initiate provisioning activities with Client and collect, review and assess the necessary information relating to the MDR Essential service and operating environment as necessary to complete the provisioning process.
- Create a Client account in the Fusion Client portal and verify that Client has access to portal.
- Assess, configure and onboard the MDR Essential managed environment based on information and instructions provided by Client.
- Provide applicable user guides, introduce and review Client’s usage and understanding of the Fusion Client portal and implement the applicable support process and procedures.
- Verify that MDR Essential Client-side technology is functioning according to the service delivery design with endpoint data visible to the Trustwave platform. NGAV individual blocks will not appear in the Trustwave platform, but data is incorporated for content during incident monitoring and response.

Client responsibilities

- Accurately complete the provisioning questionnaire and respond to requests from the provisioning team when establishing contact and collecting the provisioning questionnaire.
- Make available an onsite resource capable of installation and troubleshooting of the MDR Essential tool(s) within Client environment.
- Provide remote access to on-premise infrastructure to accommodate remote analysis and remediation as set forth in this service description.
- Provide appropriate credentialed access to Trustwave.
- Provide and maintain a secure connection between the managed MDR environment and the Trustwave platform. Connection must be compatible with available Trustwave connection standards.
- Develop and complete a comprehensive test plan to review all impacted Client systems associated with the provisioned MDR environment prior to commencement of the onboarding process.
- Read and confirm Client's understanding all provided user guides and documentation and participate in and confirm Client's understanding of the processes explained during the welcome call.
- Review security event and alert activity in the Fusion Client portal;
- Adhere to Trustwave's recommended security practices with respect to the MDR service, including adhering to agent patch management and updates and best practices in system configuration.

Client acknowledges that:

- The Trustwave provisioning, management and threat analysis services are performed remotely. Any on-site provisioning or support services required by Client may be acquired separately as a Trustwave consulting service.
- Trustwave is not responsible for delays in provisioning due to delays or inaccurate provisioning questionnaire responses and Client provided information.
- Failure to implement and comply with Trustwave recommended security practices may adversely impact the operation and functionality of the MDR Essential service.
- Client has made its own enquiries as to the available features and functionality of the MDR Essential service and the suitability of the MDR Essential service to meet Client's requirements.
- Client will not have privileges greater that read-only access to the MDR Client-side technology Graphical User Interface.

Monitoring

Following service implementation, Trustwave monitors system health status, active log collection, and disk and data storage and availability and capacity. Anomalies identified during monitoring follow the procedures identified below:

- Analyzed events may generate alerts, which are presented to Trustwave analysts and displayed in the portal for additional investigation by Client and Trustwave.
- Trustwave security analysts will investigate events and alerts in the local SIEM environment; no log data is transferred to Trustwave.
- Trustwave analysts review the generated alerts, collected events, and trends of activity to identify any suspicious behavior in the environment. If suspicious activity is found, a ticket is generated, Client is notified through the incident response process defined with Client, and the ticket information is displayed in the Trustwave portal.
- Alerts that are determined to be a potential security threat and are of a high severity are emailed to Client and followed up by a phone call, following Client's pre-defined escalation procedures.
- Alerts that are determined to be a potential security threat and are of a low or medium severity are emailed via ticketing system to Client following Client's pre-defined escalation procedures.
- Trustwave provides 24x7 telephone and email support.

- Trustwave shares findings through the Fusion visualization tool for reports and interactive features that are related to service components.

Client-side technology (EDR & NGAV application) maintenance

Trustwave will monitor the need for EDR updates.

- The EDR application will be maintained by Trustwave.
- The NGAV application will be maintained by Trustwave.
- Client will provide Trustwave GTO with appropriate non-root access for maintenance and service execution activities of on-premise EDR application.
- Client will be responsible for updating endpoint sensors (light agents) upon the recommendation of Trustwave in a timely fashion.
- Application and sensor updates will:
  - Be assessed to determine the level of severity.
  - Be executed during maintenance windows designated by Trustwave (dependent on severity; exceptions coordinated with Client). Considerations can be made to accommodate Client's best maintenance opportunities with the understanding that maintenance windows are required and necessary to maintain the managed system, not an optional component of the service.
  - Require current, valid software licenses which may include subscriptions to threat intelligence or IOC feeds.

Trustwave responsibilities

- Monitor connectivity status of endpoints managed by MDR Essential MSS managed environment.
- Provide product and security updates for Client agents.
- Manage EDR application maintenance applicable to the MDR Essential service in order to provide timely updates, prioritized by the nature of the update as it applies to the MDR Essential service.
- Provide service-related remote assistance, support and configuration within the MDR Essential managed environment.
- Attempt to resolve any connectivity or system issues identified in order to return the MDR Essential service to a steady state of operation.
- Schedule and test required application updates with Client through the predefined ticketing system.

Client responsibilities

- Inform Trustwave of all Client environment maintenance activity and changes that may impact Trustwave's ability to provide the MDR Essential service, as designed.
- Provide, when necessary to Trustwave, access to vendor portals to allow for software and license downloads and provide necessary authorizations for Trustwave to act on behalf of the Client for management and maintenance purposes.
- Access the Fusion Client portal, respond to tickets and confirm scheduled implementation of product updates and security updates.
- When requested by Trustwave, provide onsite support for the MDR Essential service to resolve connectivity or other support issues.
- Client acknowledges that the implementation of necessary product updates is not an optional feature of the MDR Essential service and failure to implement a required product update may adversely impact the operation and functionality of the MDR Essential service.

Additional and related services

Depending on existing contracts and consulting services in place, Trustwave can manage the deployment and patching of the EDR server as well as the endpoint agents through an additional service.

Depending on the technology selected for the MD or MDR service, additional service statements of work will be required. All MDR opportunities must also have a tier of MD associated with the deployment for managed detection.

Proactive threat hunts, digital forensics and incident response engagements are not included as part of the MDR Essential service, but are available for purchase as a separate services.