SERVICE DESCRIPTION

Managed Detection and Response Complete (MDR Complete)

Overview

The Trustwave Managed Detection and Response (MDR) Complete service provides 24x7x365 monitoring of detection and response tools, coupling automated, technology-based detection, analysis and response with Proactive and Continuous Threat Hunting, Data Forensics, and Incident Response and Remediation.

Base Features of Service

Features overview

The MDR Complete Service includes the following basic service features:

- Proactive and Continuous Threat Hunting
- 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
- Digital Forensics Investigations
- Incident response (IR) retainer
- Nine global SOC's and +250 security professionals
- Health, status and availability systems management using the Fusion platform
- Easy to access reporting of IR and containment actions from the Fusion platform

Security Threat Analysis, Investigation & Response (Remediation)

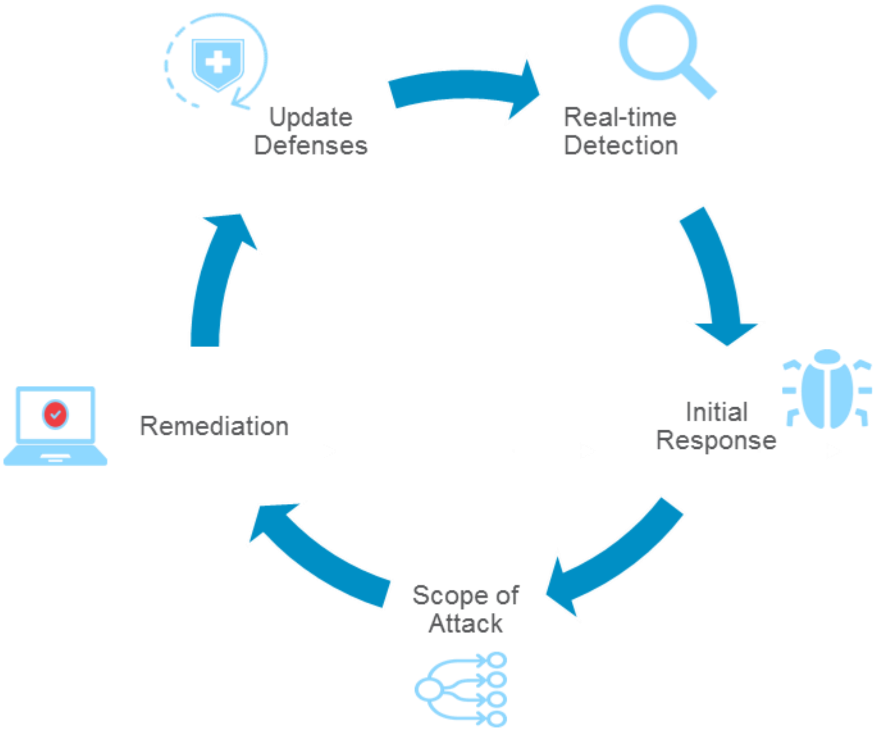
Overview

Security Threat Analysis, Investigation & Response (Remediation) includes monitoring and investigation to determine what level of risk exists and what the appropriate, predefined response (remediation) should be. MDR Complete leverages Trustwave's global scale and deep security expertise with advanced behavioral analytics & real-time threat intelligence to monitor endpoints and detect & remediate malicious activity, including pre-emptive Threat Hunting. With client coordination, the SOC Team employs additional incident investigative and response services (such as Trustwave SpiderLabs IR) to combat advanced attacks.

Continuous protection process

MDR Complete encompasses a five-phase process to provide continuous protection against advanced threats:

- Detection: Analytics with multiple & unique threat intelligence feeds analyze endpoint behavior with a focus of IOC’s that may involve memory injections, executables, files changes, and registry modifications.
- Initial Response: On potential signs of compromise, MDR Complete moves to isolate questionable activities to include locking accounts, killing processes, and quarantining affected systems.
- Scope of Attack: Analysis and investigation in this phase include understanding the where, what, when, and how of the threat. This phase identifies any lateral movement within an environment as well as other suspect activities (such as network communications).
- Remediation: With a clear understanding of the scope of attack, the SOC is able develop and execute an effective remediation plan.
- Update Defense: Once the threat has been remediated, this phase accounts for an actionable plan to protect the environment from future similar threats.



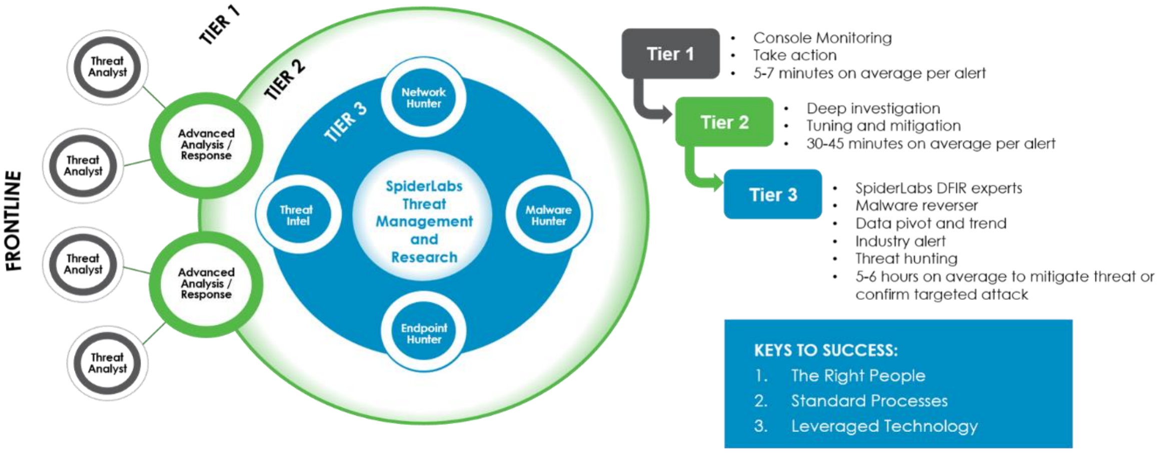
Continuous Protection Against Advanced Threats

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. Each investigation leverages Trustwave’s significant global security experience and industry best practices, to include knowledge gained from the activities involving Trustwave Spider Labs Malware Research, Threat Intelligence, and Incident Response teams. MDR Complete leverages a three-tiered approach to addressing Incident Response:

- 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 EDR solution for investigation. Clear threats are remediated, when possible. Investigated potential threats are escalated to Tier 2.

- The Trustwave SOC Tier 2 (Advanced Analysis/Response) provides deeper analysis with most threats remediated by this point (30-45 minutes on average per alert). Tier 2 activities include accessing available information from other client specific data sources, external data sources or captured malware to understand more clearly the nature of the attack and the potential danger to the client.
- The Trustwave SOC Tier 3 (Threat Management and Research) leverages Trustwave's SpiderLabs team for advanced analysis and remediation should deeper analysis should be required. Tier 3 will spend up to 6 hours leveraging advanced capabilities (such as malware reverse engineering) to get to the heart of the threat. At this point, the malicious activity is either resolved or the service will have identified the need for more intensive investigation to remediate the issue. In the latter case, the customer will be advised that a DFIR Consulting engagement will be necessary to combat the attack. The determining factors that may prompt a DFIR Consulting recommendation include:
    - Indications of APT type behavior – significant lateral movement utilizing multiple malicious tools.
    - Evidence of an active attacker on the network and altering tactics to bypass security mechanisms.



Tier 1
- Console Monitoring
- Take action
- 5-7 minutes on average per alert

Tier 2
- Deep investigation
- Tuning and mitigation
- 30-45 minutes on average per alert

Tier 3
- SpiderLabs DFIR experts
- Malware reverser
- Data pivot and trend
- Industry alert
- Threat hunting
- 5-6 hours on average to mitigate threat or confirm targeted attack

KEYS TO SUCCESS:
1. The Right People
2. Standard Processes
3. Leveraged Technology

Trustwave's Tiered Approach to Incident Response within MDR for Endpoints

Trustwave's proprietary threat analysis engine, leveraged by the SOC Teams, considers all available client security and infrastructure information to identify potential indications of security attacks and attempts to compromise client systems.

- All security events are collected, assessed and stored for a defined period time to assist with potential future analysis.
- Potential incidents identified by the automated analysis engine are further investigated by Trustwave SOC analysts immediately.
- Other security events collected but not identified by the automated analysis engine are maintained to assist in potential future investigations.

Proactive threat hunting

Proactive Threat Hunting is performed as a part MDR Complete at the onset of service:

- Threat Hunting activities on a proactive basis may find lurking, dormant threats before breaches occur.
- Threat Hunting may be performed as IOC's can be identified and applied to supported technologies within the service.
- IOC's are identified through the research activities leveraging SpiderLabs intelligence original research and threat activities found through threat services being delivered through the global threat operations team.
- Any incident response activity resulting from Threat Hunting activities will follow the established IR Protocol as defined per client.

Incident notification protocol

This protocol defines the client's notification preferences (i.e., notification about confirmed incidents only or all suspicious alerts). The Trustwave 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 and escalated to the IR analyst.
- The IR analyst has confirmed the incident is breach or malware activity and is implementing IR protocols.

Incident response protocol

Once an incident has been confirmed the IR Analyst during the IR investigation process, the analyst will implement pre-approved response actions. The IR protocol is established during the provisioning process to document authorization for response activities authorized by the IR analysts.

- The Response Protocol is stored within the Trustwave portal and always available to the customer and Trustwave IR analysts for reference.
- The absence of a Response Protocol will be assumed that no response actions have been authorized without prior approval through normal change request and incident notification processes.
- Any changes to the IR protocol must be submitted by the policy contact and follows the policy change request SLA. The following represent response actions that are available depending on the solutions capabilities (some EDR solutions offer slightly different response actions):

Response option	Description
Process blacklisting Or hash Ban	Implementing a ban on a file hash or updating a process blacklist
Endpoint quarantine	Restricting network access to the endpoint to only the IR endpoint management infrastructure

Initiate interactive session on endpoint	Enable analysts to open a command shell on the endpoint system
Download files to endpoint	During the IR investigative process downloading tools may be necessary to contain the breach or capture necessary information
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) the client's endpoint environment as outlined in the MDR Complete service.
- Manage the process in developing a Client Runbook that will outline the client priorities and approved response actions that may be executed by Trustwave on the 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 Complete service deployment & execution. Fusion Portal will also be used a repository for the 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, the 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 timeframe 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.

Tool Selection and Client access model

Tools are selected and licensed by the customer. Tool selection may include EDR, NGAV, or XDR technologies. Tools will be configured for read only access by the customer.. The Fusion Client Portal will be the primary client interface to track and manage MDR Complete MSS activities. Fusion Client Portal provides access to:

- View current & historical security data and posture information across managed environment (MDR Complete and other enabled Trustwave Managed Service 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 of provisioning progress.

Provisioning and Implementation

Overview

Service Provisioning outlines the activities required to establish the MDR Complete managed service between Trustwave and the client. The execution of Service Provisioning can be divided into two phases: Client-Side Implementation and Trustwave SOC Onboarding Process.

Client-side implementation

This is the technology implementation of the tools required to send client endpoint information into the Trustwave SOC:

- Client-side Implementation phase involves the planning and implementation of the technology (known as the Endpoint Detection & Response or EDR solution, coupled with NGAV if selected by customer) and either 1) a hardware or virtual Log Collection Appliance (LCA) or 2) an on-premise Trustwave 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 in a manner that Trustwave can meet service responsibilities and SLA's. (Trustwave will not assume responsibilities described for this service until all relative capabilities of the EDR solution are demonstrated to be functioning properly with required access privileges in place.)
- This phase includes the implementation of sensors (light agents) on each endpoint as well as EDR management software (dependent on technology solution) which could 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 of technology solution).
- Execution of client-side provisioning from the Trustwave side will be led by Trustwave Provisioning, the customer, or the EDR Technology Solution Partner Services Team.

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 the client-side EDR solution into the Trustwave SOC. NGAV alerts are not included into this data stream to Fusion platform. Once the client data is successfully directed into the Trustwave SOC, the

SOC team begins a “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 be generating significant amounts of inconsequential/irrelevant data.
- Partnering with the 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 – The Client Contact facilitates the change control process for all managed systems as well as the appropriate notification of security incidents. The customer portal provides levels of access that can be leveraged by clients 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 the 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 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 customer portal and leverages the security & 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 portal support assistance from the SOC.
        - Assign and interact with security incidents within the portal.
        - Request configuration changes because of a security investigation (These changes must be approved by a policy contact and the change request details stored in the Fusion 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:
            - Clients employed incident response activities may be defined.
            - In the event that some activities may require collaboration with client resources (such as the 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, isolate 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 & Response (Remediation)”.

Trustwave responsibilities

- Navigate the Client through the provisioning process until the SOC has ongoing management control of the MDR Complete environment.
- Initiate provisioning activities with Client and collect, review and assess the necessary information relating to MDR Complete 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 onboarding the MDR Complete managed environment based on information and instructions provided by Client.
- Provide applicable user guides, introduce and review the Client’s usage and understanding of the Fusion Client Portal and implement the applicable support process and procedures.
- Verify that MDR Complete 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 Complete within the client environment.
- Provide remote access to on premise infrastructure to accommodate remote analysis and remediation as defined by this service description.
- Provide appropriate credentialed access to Trustwave.
- Provide and maintain a secure connection between the managed MDR Complete 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 customer systems associated with the provisioned MDR Complete environment prior to commencement of the onboarding process outlined in this service description.
- Read and confirm the Client’s understanding all provided user guides and documentation and Participate in and confirm the Client’s understanding of the processes explained during the welcome call.
- Review Security Event and Security Alert activity in the Fusion Client Portal;
- Adhere to Trustwave’s recommended security practices with respect to the MDR Complete service, including adhering to agent patch management and updates and best practices in system configuration.

The Client acknowledges that:

- The Trustwave provisioning, management and threat analysis services are performed remotely. Any on-site provisioning or support services required by the 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 or Endpoints managed service.
- It has made its own enquiries as to the available features and functionality of the MDR Complete and the suitability of the MDR Complete service to meet the Client’s requirements.

- Client will not have privileges greater that read-only access to MDR Complete client-side technology implementation to execute the MDR Complete service.

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 Security Operations Centers (SOCs) located strategically across the globe to provide for services. The SOC analysts are responsible for the 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 above). Configuration change requests can be made through the following methods:

- Fusion 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 service 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 MDR Complete:

- On-premise servers will be maintained by the customer.
- The customer retains root access and is responsible for all system-related maintenance.
- The on-premise server will be solely dedicated to the hosted EDR & NGAV application (if enabled).
- With the exception of emergency activities, maintenance of the on-premise server will be coordinated with Trustwave 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 & 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.

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.

- Customer will provide Trustwave GTO with appropriate non-root access for maintenance and service execution activities of on-premise EDR application.
- Customer 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 customer'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 Complete MSS managed environment,
- Provide product and security updates for client agents.
- Manage EDR application maintenance applicable to MDR Complete service to provide timely updates prioritized by the nature of the update as if applies to the MDR Complete service.
- Provide service-related remote assistance, support and configuration, within the MDR Complete managed environment.
- Attempt to resolve any connectivity or system issues identified in order to return the MDR Complete service to a steady state of operation.
- Schedule and test required application updates with the client through the predefined ticketing system.

Client responsibilities

- Inform Trustwave of all client environment maintenance activity and changes that may impact on Trustwave's ability to provide the MDR Complete service, as designed.
- Provide, when necessary to Trustwave, technician, 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 Complete service to resolve connectivity or other support issues.
- Access the Fusion Client Portal, respond to Tickets and confirm scheduled implementation of Product Updates.
- The Client acknowledges that the implementation of necessary Product Updates Update is not an optional feature of the MDR Complete service.
- Failure to implement a required Product Update, may adversely impact the operation and functionality of the MDR Complete service.