eSENTIRE

Service Description:
Endpoint Services – CrowdStrike

1. Service Overview

eSentire's Managed Detection Response for Endpoint Services - CrowdStrike (the "**Service**") is a managed service providing endpoint-level visibility and control to support threat prevention, threat detection, investigation, and response leveraging the CrowdStrike Falcon® agent/license ("**Agent**") installed on servers, laptops, and desktop devices with supported operating systems within Client's environment (the "**Client Environment**").

The eSentire Atlas Platform will capture telemetry from in-scope endpoints, enrich signals from other sources, analyze for suspicious or threatening behavior and support eSentire's Security Operations Center ("**SOC**") in delivering prevention, appropriate investigations, response, and remediation (as appliable, pursuant to the ordered subscription type). The Prevent subscription allows for automated identification, prevention, and remediation of threats via the Endpoint Agent. The Detect and Respond subscription allows for full endpoint telemetry visibility to give the SOC analysts the ability to identify and investigate potential threats or suspicious activity. Client also has the option to add on Identity services (as further described below). Any subscription level selected by Client is supported by eSentire's SOC on a 24x7x365 basis.

2. Service Definitions

Any capitalized terms contained in this Service Description are as defined herein, or as defined on the Managed Detection Response ("**MDR**") Services landing page (https://www.esentire.com/legal/documents?Service=MDR), referred to herein as the "**MDR Landing Page**").

3. Service Capabilities

3.1. Investigation, Analysis and Response. eSentire is responsible for security event analysis and investigation to determine if a security event is real and warrants an escalation to Client and potential response action (isolation). If an event is deemed Actionable, due to its behavior and the type of detection, it will be escalated to Client as an Alert. Malicious activity will be contained (isolated) immediately by eSentire once identified. The SOC will perform event triage, assign criticality, and include all supporting information within the Alert and, if necessary, initiate escalation to Client.

eSentire will investigate all security events identified during the Service and escalate Actionable Alerts as appropriate. Once investigated, events are classified, alerted, and escalated to Client if there is an action required. eSentire will utilize an escalation process mutually agreed upon between Client and eSentire during the on-boarding process, to contact and relay information to Client. It is eSentire's responsibility to classify the criticality of the Alerts derived from individual events as part of the Service.

4. Subscription Types

4.1. Subscriptions. Client can subscribe to any of the following Service subscriptions both available to ensure complete endpoint coverage ("**Subscription**"), and are further described below:

4.1.1. Endpoint Services – CrowdStrike – Prevent Subscription:

This Subscription relates to the implementation of Next-Gen AV (NGAV) capabilities such as policy and configuration-based prevention mechanisms within the Endpoint service. This includes but is not limited to the ability to block, kill, or quarantine attempted malicious code execution and malicious running processes. This Subscription option includes:

- detection and prevention events monitored by the eSentire SOC
- known and unknown malware and ransomware detected by using machine learning (ML) and artificial intelligence (AI)
- behavior-based indicators of attack (IOA) prevent sophisticated file-less and malware-free attacks
- the execution and spread of threats via unpatched vulnerabilities stopped by exploit blocking
- activities known to be malicious blocked by threat intelligence prevention

4.1.2 Endpoint Services – CrowdStrike – Detect and Respond Subscription:

This Subscription relates to the implementation of threat detection on data such as file monitoring, process command-line parameters, process monitoring, process use of network, loaded DLLs, API monitoring, binary metadata, windows registry monitoring from Client's endpoint. This component of the Service gives eSentire full spectrum visibility into the endpoint and allows for hunting for specific threats. This Subscription option includes:

- detections investigate and respond to by the eSentire SOC
- full spectrum visibility at the endpoint provided by continuous raw event recording
- enabled threat hunting—proactive and managed—with full endpoint activity details
- enabled entire attack life cycle visibility with context and threat intelligence data
- situational awareness of the current threat level of the organization, and how it is changing over time.

4.2 Identity Services. Client may also choose to subscribe to identity services leveraging a license to CrowdStrike's Falcon Identity ("**Identity Services**"), on Agents deployed as part of the Subscription option(s) described above, and as required below. This subscription relates to the initialization and configuration of the Falcon Identity Threat Protection module, and integrations with supported Identity providers. The Service will collect information in the Client Environment. The Endpoint Agent collects data from Active Directory on the installed Domain Controller. If Client orders Identity Services as part of the Service, it will include the support as detailed in Table 1, and it will enable the following:

- Provides the SOC additional visibility, and ability to monitor and investigate the scope and the impact of access privileges for identities across Clients Active Directory (AD) and Azure AD.
- Delivers AD security posture overview by analyzing user behavior and risk changes over time, including increases in account lockouts, high-risk endpoints and duplicate/compromised passwords to get an overview of the attack surface of the organization.
- Streamlines identity verification and conditional access policies, leveraging adaptive analysis based on authentication patterns and behavior baselines.
- Extends multi-factor authentication to legacy systems and tools, reducing attack vectors.

The Idnetity Service is only offered in conjunction with the following Endpoint Services – CrowdStrike Subscriptions, either:

- Endpoint Services – CrowdStrike - Detect & Respond; or
- Endpoint Services – CrowdStrike - Prevent AND Endpoint Services – CrowdStrike - Detect & Respond (purchased together).

4.3. Third Party License Requirements. Client may request each Service Subscription to be provided by eSentire as a fully managed service ("MSSP"), or in a managed only capacity ("Managed Only"). Licensing requirements for each are detailed below:

4.3.1. MSSP Licensing requirements:
eSentire will procure all required licensing directly from CrowdStrike.

4.3.2. Managed Only Licensing requirements:
The Service option requires that Client secures appropriate endpoint licensing with CrowdStrike. The endpoint license count maps to an entitlement of log ingestion expressed in GB/day. See Order Form for details. Client must procure and maintain endpoint licensing ("License") with CrowdStrike, during the entire Term of the Service, and coordinate proper licensing permissions with the Product Publisher to allow eSentire full administrative access and credentials into Client's License instance. Client must purchase the following applicable licenses:

- CrowdStrike Falcon Insight XDR (Required for the Detect & Respond Subscription option)
- CrowdStrike Falcon Identity Threat Protection (Identity Services)
- Threat Graph Standard (Required for all Subscription options)
- CrowdStrike Falcon Prevent (Required for the Prevent Subscription option)

Client will retain ownership of the License and will continue to have all access to utilize their endpoint License. Client acknowledges and agrees that any changes made by Client in the licensed environment could negatively impact eSentire's ability to deliver the Services. In addition, Client acknowledges and agrees that any changes made by Client during the term of this Service should be reviewed with eSentire, otherwise eSentire shall be released from any and all obligations to effectively provide the Services as contemplated herein. Throughout the Term of the Service, Client must provide and eSentire must maintain administrator or equivalent access which enables eSentire staff and systems to execute

5. Response Actions for Identified Threats

If Client has ordered the Prevent Subscription, once moved to a service-ready state, the Agent will be configured to execute any of the following actions on detection of confirmed malicious threat:

- process or file denylisting on the endpoint;
- block and kill malicious processes; or
- detect and prevent known/unknown bad software (quarantine).

If Client has ordered Identity Services, once moved to a service-ready state, the platform will be configured to execute any of the following actions:

- enforce Multi-Factor Authentication on users based on Client-approved conditional access policies; or
- restrict user access based on Client-approved conditional access policies.

If Client has ordered the Detect and Respond Subscription, following the successful identification of a confirmed threat targeting Client's Environment, the eSentire SOC will utilize the Service to execute one of the following actions:

- endpoint isolation;
- initiate interactive session on endpoint;
- download files to endpoint;
- delete files on endpoint; or
- gather files and memory for host.

If Client has purchased other eSentire services, response may be implemented at multiple enforcement points, including but not limited to network, endpoint, and cloud (if applicable).

Unless Client opts-out, as part of the Endpoint Services – CrowdStrike - Detect & Respond subscription option, eSentire will isolate potentially compromised machines. eSentire will isolate the machine using the this Subscription and notify Client of the isolation via the agreed upon escalation procedure including evidence to support the action. The machines will remain in isolation until the threat has been remediated or Client has accepted the risk and has requested the eSentire SOC to remove the host from isolation.

- All endpoint Detect and Respond Agents are considered authorized for isolation unless otherwise communicated by Client.
- eSentire will escalate all Alerts that require isolation to Client for visibility and active feedback on the Alert. Client commits to identifying critical assets that are NOT to be isolated unless Client has given written authorization.
- eSentire commits to isolating machines that are NOT on the unauthorized list only to prevent the spread of malicious code and lateral movement by suspected attackers.

Clients subscribed to Endpoint Services – CrowdStrike - Detect and Respond subscription are hereby advised that the eSentire SOC has the functionality to isolate machines on Clients' network, the ability to use this function to protect the network, and that the isolated machines will lose all connectivity to all other devices or resources on the network. eSentire is limited to endpoint response actions through the Agents powered by this Detect and Respond Subscription.

5. Incident Alerts and Reporting

eSentire sends Alerts via email for medium, high, and critical severity events followed by escalation(s) for high and critical severity events, as necessary, based on agreed upon escalation procedure in the configuration worksheet. A member of the eSentire customer success team will be assigned to review the overall Alerts with Client. All Alerts are available within the Insight Portal for Client review. All reporting is delivered through the Insight Portal.

6. Deployment

eSentire is responsible for providing Clients with the required installation documentation for the Agent. eSentire will provide an expert deployment engineer resource during deployment of the Service to assist with questions around how to deploy and the requirements for the Service.

For each of the Service Subscription options (including: Prevent, Detect and Respond, and Identity Services) deployment methodologies can take up to 30 days to fully tune. eSentire, working with Client, requires that at least 80% of Client contracted endpoint quantities have Agents installed and/or deployed to be able to complete the tuning process and move to production-ready state. Once tuning has been completed it is transitioned to the SOC for real-time monitoring, and the Service is considered fully deployed and in-production.

Once the Service is moved to an active state, eSentire will provide the following documents:

- complete list of machines that are active within the Service; and
- detailed summary of activities investigated during deployment.

7. Tuning and Configuration

eSentire is responsible for configuring and tuning the Services. Endpoint Services – CrowdStrike – Prevent subscription, requires a special configuration and tuning process due to the automated blocking/killing

capabilities. Detections through the Prevent Subscription capability are handled by an eSentire's deployment engineer during the tuning and configuration period(s). All detections via the Endpoint Services – CrowdStrike – Detect and Respond subscription capability are handled by the eSentire SOC immediately upon Agent install.

7.1. Endpoint Services – CrowdStrike - Prevent Subscription. Summary of the tuning and configuration for this subscription option is as follows:

- The configuration of the Prevent Subscription is a phased approach to increase the security of the prevention component.
- Requires 80% of the Agents to be deployed to the infrastructure before configuration and tuning begins.
- Upon successful installation to 80% of the infrastructure an eSentire deployment engineer will be assigned.
- Weekly meetings to take Client through configuration and tuning will happen over a four week period.
- Once Client is in a hardened state, the Service is transitioned into production monitoring by the eSentire SOC.

7.2. Endpoint Services – CrowdStrike - Detect and Respond Subscription. Summary of the tuning and configuration for this subscription option is as follows:

- Data required for detection begins streaming immediately after installation of the Agent.
- eSentire SOC begins monitoring detection events immediately after installation.
- A baseline period of four weeks begins once 80% of Agents are installed.

7.3 Endpoint Services – CrowdStrike – Identity. Summary of the tuning and configuration for this subscription option is as follows:

- The configuration of the Identity Service is a phased approach meant to harden the security posture of an environment.
- Network Traffic Authentication Inspection must be enabled.
- Required 100% of the agents to be deployed to the domain controllers before the baseline period (30 days) ends.
- After the baseline period, eSentire will work with Client to identify any misconfigurations and perform a review of domain security posture.
- Once Client is in a hardened state the service is transitioned into production monitoring by the eSentire SOC.

8. Client Responsibilities

Client will perform the obligations listed below and acknowledges that the ability for eSentire to deliver the Service is dependent upon Client's compliance with the obligations hereunder, including meeting the service levels below. Non-compliance with these obligations may result in suspension of the Endpoint service or suspension of service levels. The responsibilities of each party are also summarized in the responsibilities matrix which can be found in Appendix A.

8.1. Deployment. Client is responsible for:

- pushing out the Agent to its infrastructure and working with eSentire to confirm it is successfully installed within a reasonable timeframe (no more than 30 days);
- granting access to all data and systems required for the successful delivery of the Services;

- ensure no firewall rules or other blocking exists, as well as any other measure taken by Client, does not prevent the communication from endpoints to the Service management server;
- ensuring there is sufficient network bandwidth and access to perform the Service;
- assisting eSentire with troubleshooting related to the installation of the Agents; and
- notifying eSentire of newly added machines to the Service.

8.2. Tuning and Configuration. Client is responsible for:

- making themselves available for weekly meetings to discuss detections identified during tuning; and
- ensuring that authorized contacts remain current, including approved access and all associated information.

8.3. Investigation, Analysis and Response. Client is responsible for:

- responding to the escalated Alerts and validating the legitimacy of the content contained within the Alert;
- updating eSentire of any changes that would change the agreed upon escalation procedures;
- validate and respond to the eSentire SOC for escalated Alerts; and
- providing information and assistance during investigations conducted by eSentire when additional information is required.

9. Service Level Objectives

The ability for eSentire SOC to perform an investigation and assess whether a threat is malicious is dependent on a supported Agent being installed on a licensed host in Client's Environment. The service levels contained on the MDR Landing Page are only applicable to hosts that are licensed as part of the Service and are actively communicating with the Service.

eSentire will monitor the Service for potential threats and respond accordingly. When potentially malicious activity is identified, eSentire will perform an investigation and will respond according to the identified threat. Additional confirmation from Client may be needed depending on the information available to the analyst at the time of the investigation.

Appendix A: Responsibilities Matrix

Function	Client	eSentire
Security – Detection monitoring, analysis	I	RAC
Security – Investigation	-	RAC
Security – Notification	I	RAC
Security – Detection resolution	-	RAC
Security – Threat Intelligence integrations	-	RAC
Security – ad hoc threat sweeps for IOCs	-	RAC
Security – custom IOAs, IOCs or workflows	RA	C
System– custom alerts, dashboards, or workflows	RA	-
System – Initial product walkthroughs and/or guides	A	R
System – Deploying initial endpoints	R	ACI
System – Initial policy and environment configurations	AI	RAC
System – Post-deployment installation or host group management	RA	CI
System – User account management and administration	RA	CI
System- End user training*	R	C
Health– Data ingestion, uptime monitoring and tuning	-	RA
Health – Managing sensor updates	RA	C
Health – Performance or troubleshooting issues - MSSP	RA	RC
Health – Performance or troubleshooting issues - Managed	RA	C

R = Responsible; responsible for action and implementation. Responsibility can be shared.
A = Accountable; ultimately answerable for the activity or decision. This includes “yes” or “no” authority and veto power.
C = Consulted; typically, the subject matter experts, to be consulted prior to a final decision or action.
I = Informed; needs to be informed after a decision or action is taken.
*= Self service