esENDPOINT Detect and Respond for Carbon Black ThreatHunter Services

Definitions

esENDPOINT Agent or Agent means the endpoint software agent utilized in providing the esENDPOINT Services and as further described below.
Alert – means an event that eSentire will escalate to the Client
Emergency Incident Response - The rapid mobilization and deployment activities aimed at quickly securing Client systems and networks, providing incident response services beyond what MDR provides. Covers the full lifecycle of an incident - containing the full extent of the attack (across all attack surfaces).
Embedded Incident Response - MDR will identify and contain the attacker (within the visibility and scope of the MDR service) and provide remediation guidance to the customer.
Forensic investigation – Salvaging as much information as possible from the Client's systems and networks deemed in scope and regression analyzing that information to conclusively determine the full extent of compromised assets.
Litigation support – Any litigation support, including but not limited to expert and fact witness testimony.
Disaster recovery and business continuity planning – Assessment, execution and/or building of disaster recovery and continuity planning processes and techniques. Used to help an organization recover from a disaster and continue or resume routine business operations.
Business impact – Any quantification of the reputational, operational, compliance or financial impact to the customer's business.

Services Description

esENDPOINT Detect and Respond for Carbon Black ThreatHunter Services ("esENDPOINT Services") provide customers with endpoint-level visibility to support detection, investigation, and response. The esENDPOINT Services enable the SOC to detect and respond to threats that evade detection from endpoint protection platforms. 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 and is supported by eSentire's SOC on a 24x7x365 basis.

Service Capabilities

Investigation, Analysis and Response

eSentire is responsible for threat detection, analysis, investigation, escalation and isolation. eSentire is responsible for security event analysis and investigation to determine if a security event is real and warrants an escalation to the Client and potential response action (isolation). If an event is deemed as actionable, due to its behavior and the type of detection, it will be escalated to the 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 the Client.

eSentire will investigate all security events identified through the esENDPOINT Service and escalate actionable alerts as appropriate in accordance with the established and agreed upon Service Level Objectives ("SLOs"). Once investigated, events are classified, alerted, and escalated to the Client if there is an action required. eSentire will

utilize the escalation process, agreed upon during the on-boarding process, to contact and relay information to the Client. The defined escalation process is a mutually agreed upon process between the Client and eSentire. It is eSentire's responsibility to classify the criticality of the Alerts derived from individual events as part of the esENDPOINT Service.

Subscription Types

The esENDPOINT Service has a single subscription type: esENDPOINT Detect and Respond.

esENDPOINT Detect and Respond Subscription

- eSentire SOC will investigate and respond to detections
- Continuous raw event recording provides full spectrum visibility at the endpoint
- Enables threat hunting- proactive and managed- with full endpoint activity details
- Enables entire attack life cycle visibility with context and threat intelligence data
- Delivers situational awareness on the current threat level of the organization, and how its changing over time.

	Threat hunting	**Automated prevention**	Host isolation	Enhanced ML capabilities
esENDPOINT Detect and Respond	X		X	X

File Analysis Retrieval/Submission

eSentire utilizes dynamic and static analysis of unknown binaries and files to improve analysis, prevention, detection and response to security threats that may impact Client environments. This enables the eSentire SOC to provide more in-depth analysis and context to their investigations of potential events, as well as enhancing the detection and prevention of future events. Unless the Client opts-out, eSentire has the ability to collect files of interest relating to compromise investigations through the esENDPOINT r Service. eSentire utilizes custom sandboxes within its Threat Intelligence Unit, but in certain situations 3rd party services, such as VirusTotal, may be used to validate detections or to derive additional context and intelligence. In exceptional cases, binaries can also be analyzed in a disassembler, and portions reverse engineered in order to better understand their capabilities, locate additional artifacts on affected systems or extract C2 addresses.

Response Actions for Identified Threats

esENDPOINT Detect and Respond, following the successful identification of a confirmed threat targeting a Client environment, provides the eSentire SOC with the ability to utilize the esENDPOINT Service to execute one of the following actions:

If Client is subscribed to multiple eSentire services, response may be implemented at multiple enforcement points, including but not limited to; network, endpoint, and cloud.

Unless the Client opts-out, as part of the esENDPOINT Detect and Respond, eSentire will isolate potentially compromised machines. eSentire will isolate the machine using the esENDPOINT Detect and Respond subscription and notify the 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 esENDPOINT Detect and Respond agents are considered authorized for isolation unless otherwise communicated by the Client.

eSentire will escalate all Alerts that require isolation to Client for their visibility and active feedback on the Alert. Client commits to identifying critical assets that are NOT to be isolated unless the Client has given written authorization.

Clients subscribed to esENDPOINT Detect and Respond 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 the esENDPOINT Detect and Respond subscription.

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 the Client. All Alerts are available within the eSentire Portal for Client review. All reporting is delivered through the eSentire Portal.

Deployment

eSentire is responsible for providing Clients with the required installation documentation for the esENDPOINT Agent. eSentire will provide an expert deployment engineer resource during deployment of the esENDPOINT Service to assist with questions around how to deploy and the requirements for the service.
esENDPOINT Detect and Respond deployment can take up to thirty (30) days to fully tune. The deployment engineer, working with the Client, requires that eighty percent (80%) of the contracted agents are 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 esENDPOINT Service is considered fully deployed and in-production.

Tuning and Configuration

eSentire is responsible for configuring and tuning the esENDPOINT Detect and Respond capabilities. All detections via the esENDPOINT Detect and Respond capability are handled by the eSentire SOC immediately upon agent install.

Client Responsibilities

Client will perform the obligations listed below and acknowledges that the ability for eSentire to deliver the esENDPOINT Service is dependent upon the Client's compliance with the obligations hereunder, including meeting the service levels below. Non-compliance with these obligations may result in suspension of the esENDPOINT Service or suspension of service levels.

Deployment

Client is responsible for:

- pushing out the esENDPOINT Agent to its infrastructure and working with eSentire to confirm it is successfully installed within a reasonable timeframe (30 days)
- granting access to any and all data and systems required for the successful delivery of the esENDPOINT 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 esENDPOINT management server
- ensuring there is sufficient network bandwidth and access to perform the esENDPOINT Service
- assisting eSentire with troubleshooting related to the installation of esENDPOINT Agents
- notifying eSentire of newly added machines to the esENDPOINT Service

Tuning and Configuration

Client is responsible for:

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

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
- providing information and assistance promptly during investigations conducted by eSentire when additional information is required

Service Level Objectives ("SLOs")

- 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 IT environment. The service levels below are only applicable to hosts that are licensed as part of the service and are actively communicating with the esENDPOINT service.
- eSentire will monitor the esENDPOINT 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 the Client may be needed depending on the information available to the analyst at the time of the investigation.

Severity Priority	Description	Notification/Escalation
Low (P4)	Minor activity recorded but not alerted, and the presence of likely unwanted activity, for example, adware.	None (included within QSR Reporting)
Medium (P3)	Suspicious activity that might not be deemed malicious by itself, and malicious activity not known to be targeted.	Alert (via email) within 60 minutes of determination of the Security Event
High (P2)	Malware event, tactics, techniques, and procedure events, or events indicating targeted attack with potential for widespread impact.	Alert (via email) and response by containment (if not blocked by prevention mechanism) by eSentire within 40 minutes of determination of a Security Event, followed by a phone call to Client per defined escalation procedure in the configuration worksheet.
Critical (P1)	Malware infection(s), virus infection(s), and lateral movement, or indications of targeted attack with a high potential to cause grave damage to critical assets.	Alert (via email) and response by containment (if not blocked by prevention mechanism) by eSentire within 20 minutes of determination of a Security Event, followed by a phone call to

Severity Priority	Description	Notification/Escalation
		Client per defined escalation procedure in the configuration worksheet.

Exclusions

The MDR service does not provide emergency incident response (as defined above) including but not limited to deep forensic investigation, recovery support, litigation support, disaster recovery and business continuity planning, and/or the quantification of the business impact, with respect to all customer assets, whether currently under embedded incident response or not.