SERVICE DESCRIPTION

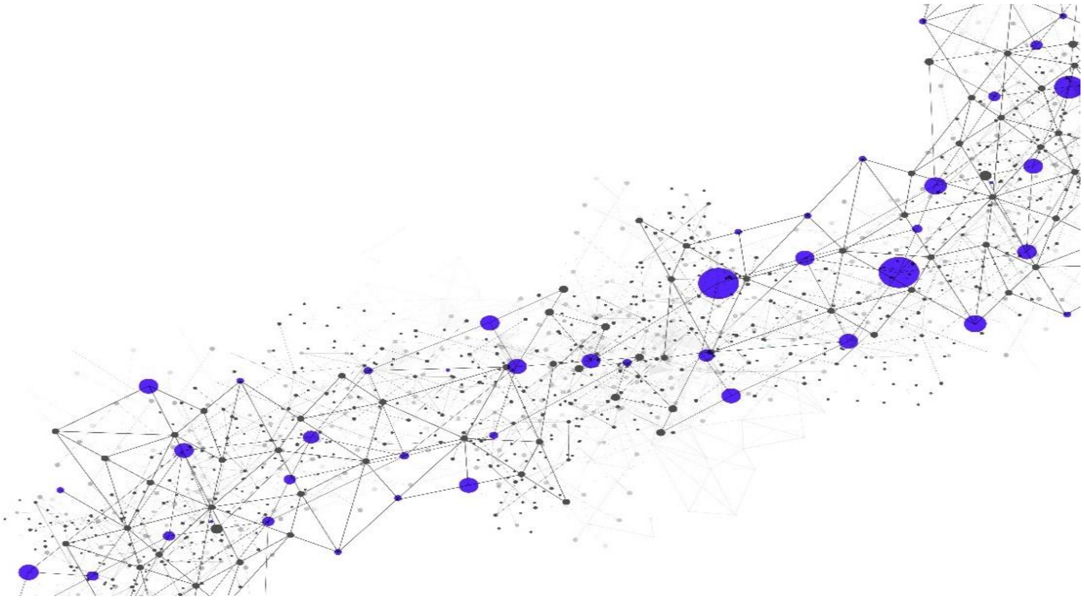
# Managed Advanced Endpoint Threat Detection with Carbon Black Response Cloud (includes monitoring)

Release Date

**June 11, 2021**

Version

**8.1**



www.secureworks.com
A Dell Technologies Company

**Global Headquarters**
1 Concourse Pkwy NE #500
Atlanta, GA 30328
Phone: +1 877 838 7947
Email: info@secureworks.com
Additional office locations: https://www.secureworks.com/about/offices

## Table of Contents

**Copyright**

This publication contains information that is confidential and proprietary to Secureworks® and is subject to your confidentiality obligations set forth in your contract with Secureworks or its affiliates. This publication and related hardware and software are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright law. Copying and/or reverse engineering of any Secureworks hardware, software, documentation, or training materials is strictly prohibited.

This publication and related Secureworks software remain the exclusive property of Secureworks. No part of this publication or related software may be reproduced, stored in a retrieval system, or transmitted in any form or any means, electronic or mechanical, photocopying, recording, or otherwise without the prior written permission from Secureworks.

Due to continued service development, the information in this publication and related software may change without notice. Please refer to your contract with Secureworks for any provided warranty information.

Secureworks® is a trademark or registered trademark of SecureWorks, Inc. or its affiliates. All other trademarks not owned by Secureworks that appear on this publication are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Secureworks.

# 1 Service Introduction

This Service Description ("**SD**") describes the Managed Advanced Endpoint Threat Detection with Carbon Black Response Cloud Service ("**Service**"). All capitalized words and phrases shall have the meanings set forth herein, as defined in the Glossary, or within the Secureworks-applicable agreement, such as the Customer Relationship Agreement.

This is a ***managed*** Service. As such, Secureworks® performs the following:

- Event stream management functions, which can include changes – e.g., Multi-Purpose Logic Engine ("**MPLE**") tuning, Red Cloak™ watchlist and suppression rule modifications), and rule/policy modifications
- Monitoring and alerting to detect event data (log) flow issues for the Service
- Managing the Secureworks Red Cloak hosted infrastructure for analyzing Endpoint telemetry

## 1.1 Overview

Secureworks will manage one or more Carbon Black Response Cloud instances (also referred to as "**Devices**" in this SD) that are licensed to Customer. Customer can procure the Carbon Black Response Cloud license from Secureworks or from a third party. The license provides access to, and use of, both the Carbon Black Management Console (also referred to as "**Management Console**" in this SD) and the Endpoint Sensor Software. Customer will install the Endpoint Sensor Software on the in-scope Endpoints that will be monitored for threats. Customer will be able to access the Management Console to view Endpoint telemetry and perform other actions.

Secureworks will monitor Security Events from Endpoints operating on systems that are compatible with the Endpoint Sensor Software from Carbon Black to detect signs of advanced threats and threat actors, search for specific indicators of compromise, maintain updated threat intelligence, analyze telemetry, and send alerts to Customer with recommendations on how to proceed should threat activity be detected. To perform these activities, Customer installs Endpoint Sensor Software on Endpoints, and the Endpoint Sensor Software sends event data to the Carbon Black Response Cloud. Then, the events are processed through the Secureworks Red Cloak Analytics System, which contains Secureworks Threat Intelligence ("**TI**"). Additional processing occurs next, through the Secureworks Counter Threat Platform™ ("**CTP**"). The processing enables detection of threats and threat actor activity that some technologies (e.g., common anti-virus software) are unable to detect. Section 2.2.1, Security Event Monitoring and Alerting, contains more information about how events are processed.

The Service allows for maintaining/storing key forensic data necessary to make threat detection and response faster and more efficient, and reducing effort required to investigate and respond to threats.

The Service includes the following components:

- Security Event Monitoring and Alerting
- Secureworks Threat Intelligence ("**TI**") Feed
- Management of Carbon Black Response Cloud
- Event Flow Monitoring and Alerting
- Software Maintenance for Devices *(applies to Customer's Carbon Black Response Cloud instance(s) only)*

See Section 2, Service Details, for more information about the Service, including further explanation of the components listed above.

***Note:*** Secureworks will not install third-party software on any appliance or system, unless explicitly indicated in Section 2 as being part of the Service.

## 1.2 Customer Obligations

Customer will perform the obligations listed below, and acknowledges and agrees that the ability of Secureworks to perform its obligations hereunder, including meeting the Service Level Agreements (“**SLAs**”) listed further below, are dependent on Customer’s compliance with these obligations. Noncompliance with Customer obligations relative to this Service may result in suspension of managed components of the Service and/or SLAs, or a transition to monitor-only components of the Service.

### 1.2.1 Endpoint Sensor Software

Customer will do the following:

- Ensure all operating systems ("**OSs**") used with the Endpoint Sensor Software are supported by Carbon Black; a list of supported OSs is located in the Carbon Black Community: https://community.carbonblack.com
- Ensure all Endpoint Sensor Software versions used are currently supported by Carbon Black; a list of supported versions is located in the Carbon Black Community: https://community.carbonblack.com
- Ensure Endpoints have sufficient available resources for installation and operation of the Endpoint Sensor Software as defined by Carbon Black’s operating environment requirements
- Install the Endpoint Sensor Software, and only on Endpoints owned by Customer as Secureworks will only deliver AETD services to such Endpoints
- Upgrade Endpoint Sensor Software as needed; use a process to deploy upgrades first in a test environment, and assess any impact before deploying software upgrades to production Endpoints and environments
- Ensure that all Endpoints to be monitored are connected to the Carbon Black Response Cloud (i.e., Endpoint Sensor Software is installed and is reporting to Carbon Black Response Cloud).
- Manage and troubleshoot the Endpoint Sensor Software, which includes the following:
  - Conduct all required ongoing maintenance of Endpoint Sensor Software
  - Ensure availability of Endpoint Sensor Software
  - Monitor performance of Endpoint Sensor Software
  - Respond to and remediate issues with availability and performance of Endpoint Sensor Software through the Carbon Black Response Cloud
  - Reinstall Endpoint Sensor Software as needed
  - Conduct all troubleshooting of Endpoint Sensor Software
  - Remove all Endpoint Sensor Software from all Endpoints and Customer’s environment by contract end or termination date
  - Ensure all Endpoints report into the Carbon Black Response Cloud at least every 30 days
    - Any Endpoint that has not communicated properly within each 30-day period will no longer be monitored and will not be included in other analytics or in the total Endpoint count

### 1.2.2 Customer-Provided License

Unless otherwise purchased through Secureworks, Customer will maintain current licensing, support, and maintenance contracts for the Carbon Black Response Cloud. Customer will also be responsible for associating Secureworks with Customer’s Carbon Black Response Cloud support and maintenance contracts to enable Secureworks to work directly with the vendor on Customer's behalf.

### 1.2.3 Licenses and Support Contract for Carbon Black

Customer can purchase AETD licenses for Carbon Black through Secureworks, and these licenses can be renewed annually. Secureworks will automatically be associated with the support contract to engage with Carbon Black on Customer's behalf. If Customer does not purchase licenses from Secureworks, then Customer will be responsible for maintaining the Carbon Black licenses including the necessary support contract. Customer will also be responsible for associating Secureworks with the support contract if Partner provides the licenses.

### 1.2.4 Connectivity

Customer will provide and maintain remote network connectivity to Customer's environment, including ensuring sufficient network bandwidth, and the in-scope Device(s) that are necessary for Secureworks to perform the Service. Customer will also allow connectivity from Secureworks IP range to Customer location(s) as applicable to the Service. SLAs will not apply to the Device(s) that is experiencing connectivity issues that are beyond the control of Secureworks.

### 1.2.5 Application Program Interface ("API") Integration

Some vendors provide APIs to interact with their systems. Any script or code creation for, usage of, maintenance of, or integration with other third-party tools are not included in this Service; Customer will be responsible for all API integration, and related activities and licenses. Secureworks will not install any third-party software applications that use the API directly on the appliance.

### 1.2.6 Communications

Customer will communicate with the Secureworks Security Operations Center ("**SOC**") through telephone (Customer-authorized representative will be authenticated) or the Secureworks Client Portal ("**Portal**") using either the ticketing interface or Chat. Customer should submit all Service-related issues or requests as tickets in the Portal or as requests through the Chat in the Portal. It is Customer's responsibility to ensure that its list of authorized representatives is up to date with the Secureworks SOC. Customer is responsible for timely responses to tickets that Secureworks escalates to Customer through the Portal.

### 1.2.7 Maintenance

Customer will notify the Secureworks SOC by submitting a ticket in the Portal or through the Chat in the Portal at least 24 hours in advance of planned Customer-side network maintenance to enable Secureworks to avoid unnecessary escalations to Customer.

### 1.2.8 Usage Overage

If, for any services identified in Customer's Service Order(s), Customer's actual usage exceeds the subscription limit of such services ("**Overage**"), then Secureworks may invoice Customer for Overage, and Customer will pay for the Overage as applicable to Customer's actual usage, from the date Secureworks identified the Overage until the end of the Services Term.

### 1.2.9 Provisioning in a Public Cloud or Private Virtual Environment

When provisioning in a Public Cloud or Virtual Private Environment, Customer will provide to Secureworks information about the environment, and may be required to make configuration changes as applicable to the Service. Customer will provide access and appropriate privileges within the environment to enable Secureworks to deploy and configure the Service.

### 1.2.10 Hardware and Software Procurement

Customer will purchase or lease the hardware and license the software necessary for Secureworks to deliver the Service. Customer will ensure that its hardware and software are at versions that are supported by Secureworks prior to provisioning of the Service and remains at versions that are Secureworks supported during the Services Term. Secureworks SLAs will not apply to platforms or versions that are End-of-Life (“**EOL**”), end of support, or are otherwise not receiving updates by the vendor or supported by Secureworks.

### 1.2.11 General

- Customer will ensure that Customer personnel are scheduled and available to assist as required for the Service(s).
- Customer will have obtained consent and authorization from the applicable third party, in form and substance satisfactory to Secureworks, to permit Secureworks to provide the Service if Customer does not own network resources such as IP addresses, Hosts, facilities or web applications.
- Customer will provide to Secureworks all required information (key personnel contact information, credentials, etc.) prior to work being started.
- Customer will promptly reply to all requests from Secureworks.
- Customer-scheduled downtime and maintenance windows will allow adequate time for Secureworks to perform the Service.
- Customer will promptly inform Customer personnel and third parties of Secureworks testing activities as needed, to prevent any disruption to Secureworks business and performance of the Service (e.g., takedown requests, ISP blacklisting).
- Customer will ensure Customer’s systems on which the Carbon Black Response Cloud will be operating have sufficient available resources as defined by Carbon Black’s operating environment requirements.
- Customer will manage file lists and policy rules for applying process disruption.
- Before requesting a process ban or disruption, Customer will ensure the process is correctly identified and not required by the Customer’s business. It is entirely Customer’s responsibility to ensure the validity of the request before submitting to Secureworks.
- Before requesting isolation of an Endpoint, Customer will ensure the Endpoint is correctly identified and the process of isolating that Endpoint will not negatively impact Customer’s business. It is entirely Customer’s responsibility to ensure the validity of the request before submitting to Secureworks. Each request for a ban, disruption, or isolation must be in an individual ticket submitted through the Portal.
- Customer will remediate all malware and threat actor activity (unless otherwise contracted with Secureworks through a separate SO).

## 1.3 Initial Implementation Scheduling and Points of Contact

Secureworks will contact Customer within seven (7) Business Days after execution of the Service Order (“**SO**”) to schedule the initial meeting.

Customer and Secureworks will designate respective points of contact (“**POC**”) to facilitate communication and support ongoing activities related to implementation of the Service.

# 2 Service Details

The subsections below contain details about the Service and how it will be implemented.

## 2.1 Service Implementation

The standard service implementation period begins after Secureworks reviews and approves Customer's signed SO, and ends when the Service is activated (made available to Customer for Customer's use), any Devices supporting the Service are activated, and management or monitoring of Devices is transferred to the Secureworks SOC. The subsections below explain the Secureworks implementation methodology for Managed Security Services (known as MSS Services) that is used to provision, install (if applicable), and activate the Service.

***Note:** Secureworks does not provide SLAs for completing implementation within a specified period of time; the duration of the implementation is dependent on several factors, such as the number of Hosted Counter Threat Appliances ("**HCTAs**") required (if applicable to the Service), the number of physical locations where managed or monitored Devices will be activated for the Service (if applicable to the Service), the number of physical locations where managed or monitored Devices will be activated for the Service (if applicable to the Service), complexity of Customer requirements, and the ability of Customer to provide Secureworks with requested information within a mutually agreed-upon time period.*

*Any effort that is required to upgrade software or replace hardware in support of Service implementation requirements can be performed by Secureworks through a separate SOW.*

### 2.1.1 Implementation Methodology

Secureworks will follow the Secureworks standard implementation methodology to implement the Service. The implementation methodology can be reasonably adjusted to meet Customer needs at the sole discretion of Secureworks. As part of implementation, Secureworks will help ensure Customer understands how to use the Service through collaborative meetings and training. Below is a high-level overview of the MSS implementation methodology.

- **Organize:** Start the project, document success criteria, enable Portal access, and finalize technical design of the Service
  - Secureworks will work jointly with Customer to validate accuracy of the information used to create the original SO against the actual Customer environment where Services will be performed ("Due Diligence"). As a result of Due Diligence, changes in the types (e.g., hardware make and/or model and software package or version) of equipment, the number of locations, or the quantities of equipment to be provisioned may be identified ("Identified Changes"). Customer acknowledges that (i) in order for Secureworks to provide intended Service coverage across such Identified Changes, an amended or additional SO may be required, which may include changes to scope and fees, and (ii) without such an amended or additional SO, Secureworks may only be able to provide Services as scoped, defined, and charged per the original SO. In some cases, an amended or additional SO may be required to provide the Services in the original SO. For example, an additional CTA may be required at a location that was not originally determined to be in scope.
- **Prepare:** Baseline the project schedule, identify required training, and send CTA(s) to Customer for installation; Customer provides information necessary to execute implementation for MSS Services
  - **CTA Deployment Guidelines:** For most Secureworks MSS Services, one or more CTAs will need to be installed, and will be included in the SO. The CTA is a Secureworks-proprietary Device that is used in the secure delivery of the Service for Device health and Security Event collection and transport.
    - If one or more virtual CTAs ("**vCTAs**") are to be deployed in a Public Cloud or Private Virtual Environment, then Customer is responsible for providing information to Secureworks about the Public Cloud or Private Virtual Environment, and Customer will make configuration changes as applicable to the Service. Customer must provide access and appropriate

privileges to the Public Cloud or Private Virtual Environment to enable Secureworks to manage the vCTA and configure it as applicable to the Service. See Section 2.1.2.1, Provisioning a vCTA into a Virtual Environment for information about provisioning in virtual environments.

  - Secureworks reserves the right, in its reasonable discretion, to use one or more **CTAs deployed in a Secureworks data center** (a **"Hosted CTA"** or **"HCTA"**) to communicate with Devices that Secureworks is monitoring, in lieu of deploying physical or virtual CTAs for use directly in Customer's environment. In such cases, the guidelines above pertaining to CTA deployment do not apply. A service deployment using a Secureworks HCTA design will be discussed and agreed upon during the solution scoping engagement within the Sales cycle. Service interruptions or failure to achieve the SLAs (as defined herein) will not be subject to penalty in the event of Customer's non-compliance with the above-listed CTA deployment guidelines.

- **Execute:** Complete configuration of CTA(s) and related service-enabling technology, validate ingestion of identified log source(s) if applicable, schedule and deliver foundational training, and activate services

  ***Notes:***

  - Existing Customer Devices that Secureworks will manage for Customer per an SO (i.e., the equipment is already installed on Customer premises) will be provisioned remotely with on-site support from Customer.
  - Secureworks provides telephone support to Customer for installing Equipment (i.e., Devices Customer purchases or leases from Secureworks).
  - After Customer Purchased Equipment that Secureworks will be managing is installed, Secureworks will access Customer Purchased Equipment (whether physical or virtual) remotely and perform the remaining configuration and implementation tasks, which may require a mutually agreed-upon maintenance window for downtime.

- **Rationalize:** Confirm Customer's ability to access and participate in management of the Service within the Portal; ensure ticket data quality and tuning of the Service and processes to Customer's environment
- **Accept:** Validate successful deployment of the Service and transition of Customer to steady-state operations

### 2.1.2 Service Provisioning, Installation, and Activation

**Service provisioning** consists of the initial actions that are completed in advance of implementing the Service for Customer, such as configuring and sending Devices to Customer. **Service installation** consists of physically putting in place a piece of equipment, connecting it to Customer's environment, and testing the ability of Secureworks to connect to the equipment. **Service activation** consists of Customer and Secureworks validating all Devices and components of the Service are available to Customer for Customer's use, and the Secureworks implementation team transferring Customer to the Secureworks SOC.

If provisioning Customer Purchased Equipment is part of the Service, then installation activities are also part of provisioning.

Secureworks performs the following provisioning, installation, and activation activities:

- Work with Customer to determine implementation date, and Secureworks submits license request to vendor in preparation for starting implementation on the agreed-upon date (***only if Secureworks is providing the license for Carbon Black Response Cloud***)

  OR

  After Customer obtains license for Carbon Black Response Cloud, Customer must submit a request to vendor to associate Secureworks with the product and support contracts;

Customer must create an Administrator account through the Carbon Black Response Cloud for Secureworks to use to manage Customer's Carbon Black Response Cloud instance (***only if Customer is providing the license for Carbon Black Response Cloud***)

- Create implementation ticket in Portal (for ongoing tracked communication between Customer and Secureworks during implementation)
- Schedule initial meeting (remote) with Customer and review SO (or on-site meeting for Customers in Japan, if needed) *(**Note:** Receipt of a Customer-executed SO is required prior to scheduling initial meeting.)*
- Provide Customer with access to the Secureworks Client Portal
- Collect Customer information that is necessary for implementation
- Complete provisioning and installation activities (e.g., accessing the Carbon Black Response Cloud to conduct remaining configuration tasks, configuring Devices within the CTP, and performing connectivity testing, if applicable)
- Provide any new Secureworks Customer with opportunity to participate in foundational training (see Section 2.4)
- Notify Customer (e.g., through email, telephone, or scheduled meeting) to activate the Service (***Note:** Customer and Secureworks will work together to ensure that Service is activated for in-scope Devices.*)
    - Secureworks can schedule Service activation in accordance with change management procedures communicated by Customer. Standard activations are performed during Business Hours on Business Days in the following regions: US, EMEA, APJ, and ANZ; however, activation can be performed at other times when scheduled in advance with Secureworks.
- Notify Customer (e.g., through email, telephone, or scheduled meeting) that the Service activation is complete, and Customer is transitioned to Secureworks SOC

#### 2.1.2.1 Provisioning a vCTA into a Virtual Environment

Virtualization includes various methods by which hardware resources are abstracted to allow multiple virtual machines ("**VMs**") to share a common hardware platform. This subsection explains provisioning a vCTA into a virtual environment (i.e., a Public Cloud or Private Virtual Environment), which enables delivery of Secureworks security services. See the Glossary for definitions of terms related to virtualization that are used in this SD.

If Customer has Private Virtual Environment, then Secureworks will provide Customer with an image to install on the Hypervisor in Customer's Private Virtual Environment, which is used to create the vCTA on a Guest VM. If Customer has a Public Cloud Environment, then Customer will access the Portal and complete steps to obtain the vCTA for use in the Public Cloud Environment. Depending on Customer's environment, the specific steps for installing and provisioning the vCTA may vary, and Secureworks will provide applicable information to Customer.

When provisioning the vCTA into a virtual environment, Customer is responsible for creating and supporting the underlying Guest VM. This includes all management and maintenance of the Guest VM (i.e., the Host), Hypervisor, and related hardware. See Section 2.5, Support for Private Virtual Environments, for more information about virtual environments including additional Customer responsibilities.

**Provisioning Requirements:** Customer must perform the provisioning activities when provisioning the vCTA into Customer's Virtual Environment (including a private or public cloud). Customer must also provide all required virtual hardware needed to operate the vCTA on the Guest VM. This includes vCPU(s), RAM, vHDD capacity, network interface card/adapter, and storage IOPS. Customer must also provide a Virtual Environment that supports the required network connectivity, which will enable Secureworks to manage the vCTA remotely.

## 2.2 Service Components

The subsections below contain information about the components of the Service.

### 2.2.1 Security Event Monitoring and Alerting

To provide Customer with Security Event monitoring and alerting of potential threat actors and threat activity, Secureworks will use a combination of the following:

- Secureworks Threat Intelligence ("**TI**")
- Machine learning
- Signature-based detections
- Human-based pattern identification – through ongoing research that CTU™ and SOC analysts conduct
- Long-term correlation
- Big data analytics

Secureworks aggregates and analyzes data from the above-listed sources and uses the data to conduct security activities that help Customer prevent and defend against attacks. The data from these sources enables faster detection of malicious activity, and action against the activity. As new threat activity is identified, new detectors are developed and deployed to the CTP, providing customers with protection from threat actors and threat activity.

Secureworks only monitors and alerts Customer of threat actors and threat activity using the above-listed sources (includes data from Devices or Security Events that are provisioned and maintained as part of the Service); no other sources such as Customer-created custom alerts and custom watch lists, or TI from other sources will be used. Secureworks reserves the right to change how monitoring and alerting is conducted, and conduct maintenance at any time to ensure the best quality of TI is applied promptly. Secureworks does not guarantee that Customer-created alerts will generate events that appear in the Secureworks Client Portal. Secureworks does not monitor the availability of the threat intelligence sources that are used for these Customer-created custom alerts and will not be subject to penalties associated with the Security Monitoring SLA if the sources become unavailable.

#### 2.2.1.1 Security Incident Identification Methods

Secureworks will use two methods to identify and act upon Security Incidents, as explained in the table below.

| Identification | Description |
|---|---|
| Real-Time Security Incidents | Secureworks will process all Security Events from Carbon Black Response in real-time using its proprietary Multi-Purpose Logic Engine ("**MPLE**") in order to identify patterns that may indicate malicious activity. This process includes analyzing Security Events to add additional context to activity and help reduce the number of false-positive Incidents. During processing, Security Events may be held for 10 to 40 minutes for correlation and context gathering (actual time depends on the use cases that may be matched within the CTP). Security Events that are malicious will be logged as Security Incidents, and further action will be taken, as applicable to the Security Incident. |
| Retroactive Security Incidents | Secureworks will use a combination of machine learning, look-back alerting for newly discovered threat indicators, and the Secureworks proprietary Long-Term Correlation Engine ("**LTCE**") in order to identify patterns of malicious activity over extended periods of time to generate and analyze |

| Identification | Description |
|---|---|
| | Security Incidents. Security Incidents generated from this retroactive analysis are not subject to the Security Monitoring SLA. |

#### 2.2.1.2 Security Event Prioritization and Security Incidents

When a Security Event is detected, initial correlation, de-duplication and false positive reduction is performed by the CTP correlation logic. Usually, if the Security Event is prioritized as Medium or High severity, then a Security Incident ticket is either automatically generated by the CTP or manually generated by a security analyst. Secureworks prioritizes all Security Events based on the severity levels described in the table below. Secureworks uses a default event handling policy and can provide this to Customer upon request. This default event handling policy can be reasonably customized at time of service implementation or during ongoing Service delivery at Secureworks' sole discretion.

All Security Events in normalized format are available to Customer in the Secureworks Client Portal. Depending on the prioritization of a Security Event and analysis by a security analyst, Security Events become Security Incident tickets, and Secureworks will notify Customer through electronic notification to enable Customer to act on the Security Incident.

| Ticket Severity | Description |
|---|---|
| High* | Security Events from Carbon Black Response Cloud that require immediate attention and/or represent a significant threat to a Customer asset – e.g., host infection(s); successful exploitations; and other known Tactics, Techniques, and Procedures ("**TTPs**") used by threat actors |
| Medium | Security Events from Carbon Black Response Cloud that do not require immediate attention and do not represent a significant threat to a Customer asset – e.g., process-based alerts, which is an aggregation of known malicious activity |
| Low | Security Events from Carbon Black Response Cloud that have little to no impact to a Customer asset or have been determined to be a false positive – e.g., instant messaging usage, adware, spyware, remote access software such as TeamViewer; usual recommended action is for Customer to tune security policies if applicable |

* ***Note:*** The Secureworks ticket severity of "High" includes Security Events that are commonly referred to as "Critical."

#### 2.2.1.3 Security Incident Analysis and Information

Upon determination of a Security Incident, Secureworks will conduct analysis to provide Customer with as much information as possible through the Security Incident ticket in the Secureworks Client Portal. Not all Security Incidents will have the same information available (depends on one or more detection methods) and as such, the information provided can vary between Security Incidents. The following are examples of information that will be provided:

- A description of the Security Event(s) and the activity that was identified
- A copy of the Security Event(s) including packet captures when provided by identifying Device
- Technical details on the threat or activity that was identified, including references
- Source and destination information including hostnames when available
- Additional content and context will be added, but can vary based on detection methods and the activity that is occurring

- Impact of the event on the affected asset
- Corroborating event data that correlates with the original event and is related to the affected asset
- Other assets in Customer's environment that were overtly interacted with by the threat actor that is related to the event
- Relevant Secureworks or third-party TI
- Additional contextual information related to the threat
- Recommended next steps based on the identified activity

In-depth analysis, incident response, forensics, and countermeasure implementation beyond policy changes to Devices are not included in this Service. Customer can purchase these services through a separate, signed SO or SOW.

#### 2.2.1.4 Retroactive Security Incident Investigations

Secureworks Incidents that are considered retroactive (i.e., "Retroactive Security Incidents" in the above table) are escalations developed from applying newly identified indicators to historical logs, researchers manually reviewing alerts from countermeasures still under active development (i.e., research for developing new countermeasures), and other similar processes. Researchers investigate threats and relevant details to determine Customer impact, and to develop new countermeasures.

Retroactive escalations may be related to threats still being actively researched and/or ongoing Security Incidents. As such, details related to Retroactive Security Incidents may be limited or privileged.

There is no limit on the number of Secureworks-initiated Retroactive Security Incident investigations that will be conducted for Security Incidents that are created based on Secureworks TI and external resources such as Secureworks trusted partners and OSINT.

Details that can be provided to Customer are added to the Security Incident ticket in the Secureworks Client Portal.

#### 2.2.1.5 Incident Investigations with Red Cloak

For Security Incident tickets, Secureworks performs Incident Investigation activities for Endpoint telemetry that is processed through Red Cloak Analytics and is defined as a critical threat. A threat must meet the following conditions to be considered critical: Detection of targeted malware, a threat actor operating within a Customer's environment, or the observation of tactics, techniques, and procedures associated with known threat actors. Secureworks will investigate these Security Incidents to provide Customer with the following information:

- Corroborating event data that correlates with the original event and is related to the affected asset
- Additional contextual information related to the threat
- Other assets in Customer's environment that were overtly interacted with by the threat actor
- Relevant CTU or third-party TI
- Impact of the threat on the affected asset
- Recommended next actions

An investigation is only performed for a Security Incident ticket that is automatically generated based on Secureworks TI and is defined as a critical threat. There is no limit (unmetered) on the number of investigations that will be conducted for these tickets. Details of each additional Incident Investigation are provided to Customer through the existing ticket in the Secureworks Client Portal within 24 hours of automatic ticket generation.

#### 2.2.1.6 Security Event Reporting

Customer can use the Secureworks Client Portal to create, customize, and access executive and technical level reports, and view and report on detailed, historical Security Event data.

Customer will be able to create both standard and customized reports that can be named, scheduled (one time or regular intervals), automatically emailed, or forwarded for review and sign-off for audit/approval purposes.

### 2.2.2 Secureworks Threat Intelligence (“TI”) Feed

The Secureworks Threat Intelligence feed will be used in conjunction with the Carbon Black Response Cloud instance(s) to protect Customer’s Endpoints. The Secureworks TI feed contains a list of identified domain names, IP addresses, hashes, and threat indicators that are used to conduct malicious activity. Secureworks will configure the TI feed with the Carbon Black Response Cloud instance(s) to which the Endpoints are connected. Secureworks will also monitor the availability of the feed as it pertains to the in-scope the Carbon Black Response Cloud instance(s).

### 2.2.3 Management of Carbon Black Response Cloud

Secureworks will manage Customer’s Carbon Black Response Cloud. Customer can submit requests through the Secureworks Client Portal for in-scope management activities, such as adding or removing users who have access to the Carbon Black Response Cloud Management Console. Upon request, Secureworks may provide out-of-scope technical support on a time and materials basis pursuant to a separate SO or SOW.

In addition, Secureworks will conduct troubleshooting for the Carbon Black Response Cloud.

### 2.2.4 Event Flow Monitoring and Alerting

Secureworks must be able to connect to the Device(s) using Internet Control Message Protocol (“**ICMP**”) or Secure Shell (“**SSH**”) depending on the platform type. Secureworks regularly conducts a Host Status validation on the Device(s) to confirm availability. If a failed or negative response is received from a Host Status validation, then an alert is automatically triggered, which sends an auto-generated ticket to the SOC.

Secureworks will use Event Flow Disruption (“**EFD**”) to detect data flow issues for the Service (e.g., connection between Carbon Black Response Cloud and associated storage resource or collection of telemetry fed into the hosted CTA, not data flow issues with individual Endpoint Sensor Software) that result in logs not being sent to Secureworks, improperly formatted logs, or when all logs received do not generate Security Events. When event flow issues are detected, an alert is automatically triggered, which sends an auto-generated ticket to the SOC. Secureworks will perform troubleshooting and then notify Customer about the event flow issue through a ticket in the Secureworks Client Portal.

For EFD tickets:

- Secureworks will attempt to restore event flow if the root cause is determined to be related to the Service. Secureworks will work with Customer to address backend connectivity log forwarding as related to the Service.
- If the root cause of the EFD is not related to the Service (e.g., a Customer-side network issue), then Secureworks will advise Customer to troubleshoot issues directly with Partner, or Customer will need to troubleshoot and resolve the event flow issue. Secureworks shall not be responsible for troubleshooting issues that do not directly relate to the Service, or Secureworks networks and environments.

### 2.2.5 Software Maintenance for Devices

Secureworks monitors all vendors represented on the Secureworks approved platforms list for release activities related to software patches and updates for managed Devices, which are Customer’s Carbon Black Response Cloud instance(s). Carbon Black will implement software patches and updates remotely.

When vulnerabilities are disclosed, Secureworks assesses the applicability of each disclosure (and related patch or patches, if available) to Customer's managed Devices. Secureworks will work with Carbon Black about vulnerabilities to be remediated.

## 2.3 Service Delivery

The subsections below contain information about how Service and support are delivered to Customer.

### 2.3.1 Security Operations Centers ("SOCs")

Secureworks maintains SOCs in the United States and internationally. To provide Service to Customers around the world, Secureworks administers security services and support from these SOCs, such as monitoring Security Events, aggregating and correlating data, conducting analysis, escalating Security Events, and performing other security-related activities. Contact information for SOCs will be provided to Customer.

### 2.3.2 Business Days and Business Hours

Business Days for Secureworks global headquarters are Monday – Friday and Business Hours are 8 a.m. – 5 p.m. US Eastern Time, excluding US holidays. Business Days and Business Hours for all other Secureworks locations vary according to local time zone and country. The Secureworks SOC is available 24 hours a day, 7 days a week, for questions and support. During non-Business Days and Hours, some SOC inquires may be sent to other support groups to address during Business Days and Hours.

### 2.3.3 Service Location(s) and Languages

The Service will be delivered remotely from a Secureworks location(s). Voice and email support are provided in English only, except in Japan where support is provided in both English and Japanese. Other components of the Service that are visible to Customer (such as reports, documentation, and the Portal) are provided in English only. Additionally, Secureworks requires that inputs and interfaces to the Service, including but not limited to logs, Application Programming Interfaces ("**APIs**"), and Command Line Interfaces ("**CLIs**"), be provided in English. Service options and availability may vary by country; contact Secureworks sales representative for details.

### 2.3.4 Service-Enabling Technology

Customer will be provided with access to the Secureworks Client Portal and the Secureworks Mobile Application ("**Mobile Application**"). Customer's use of the Mobile Application shall be subject to the terms and conditions set forth in the Mobile Application. In addition, one or more CTAs will be provisioned. Below are explanations of these items.

#### 2.3.4.1 Secureworks Client Portal

The Portal is the online site for all Managed Security Services Customers, and provides the following:

- Visibility to Customer's Secureworks Services
- Ability to submit tickets to Secureworks with concerns or issues relating to Managed Security Services
- Monitor events and escalations generated
- Access the Secureworks Learning Center (training and self-education – webinars, documentation, SDs, Portal-specific features, and related content)

Access to the Portal is enabled for Customer-specified authorized users during the Organize phase of service implementation (see Section 2.1.1 for more information), and training regarding Portal use is conducted during the Execute phase of service implementation. It is

Customer's responsibility to ensure that access for authorized users of the Portal remains current.

All information received by Customer through the Portal is solely for Customer's internal use and may not be re-distributed, resold, or otherwise transmitted outside of Customer's organization.

2.3.4.2 Secureworks Mobile Application

The Service is integrated into the Mobile Application. As part of Consultation, Customer and Secureworks will review Customer roles and access to Service features in the Mobile Application. All information received by Customer through the Mobile Application is solely for Customer's internal use and may not be re-distributed, resold, or otherwise transmitted outside of Customer's organization.

2.3.4.3 Counter Threat Appliance

The Service requires one or more hosted and/or virtual CTAs ("**HCTA**" or "**vCTA**", collectively referred to as "**CTAs**") to communicate with Customer-Side Technology (e.g., for data collection and transfer for monitored Devices). CTAs should be provisioned in advance of Service Commencement Date and meet minimum hardware and version requirements.

### 2.3.5 Customer and Secureworks Responsibilities

The responsibility assignment matrix below describes the participation required by both Customer and Secureworks in completing tasks or deliverables for a project or business process to facilitate successful service delivery. Secureworks uses standard RACI role criteria for managing Customer projects and deliverables. These roles are defined as follows:

- R – Responsible: Role(s) assigned to do the work. For any individual task, there could be multiple roles responsible.
- A – Accountable: Role(s) that make the final decision and has ultimate ownership.
- C – Consulted: Role(s) consulted as the subject matter expert ("**SME**") before a decision or action is taken.
- I – Informed: Role(s) updated with status of work being done, status of ongoing work, and results of work completed.

***Note:*** The SOC provides Quick Start guides to Customer, which contains more detail about SOC-specific roles and responsibilities.

| **AETD Carbon Black Response Cloud** | | | |
|---|---|---|---|
| **Activity** | **Task** | **Customer** | **Secureworks** |
| **Service Preparation** | Provide contact information for authorized contacts regarding Customer's account | R, A | I |
| | Provide information for authorized users who need access to the Portal (Customer will modify as needed at any time through the Portal, and add / remove users as needed) | R, A | I |
| | Provide shipping information for Secureworks to send physical Devices required to implement Service | R, A | I |
| | Create and provide to Secureworks the escalation procedures to follow for tickets | R, A | I |

| AETD Carbon Black Response Cloud | | | |
|---|---|---|---|
| **Activity** | **Task** | **Customer** | **Secureworks** |
| | (Customer will modify as needed at any time through the Portal) | | |
| | Enter Customer's initial escalation procedures into Portal | A, C, I | R |
| | Provide information on support requirements, sizing recommendations and sample deployment scripts (applicable to Public Cloud Environments only) | I | R, A |
| | Provide to Customer the implementation guidelines for service implementation | I | R, A |
| | Ensure Endpoints meet Secureworks-provided hardware and software specifications prior to the start of implementation | R, A | C, I |
| | Verify that the Endpoint or environment in which the Endpoint Sensor Software is being installed meets the specifications of the vendor for the Endpoint Sensor Software prior to the start of implementation | R, A | C, I |
| | Prepare the environment as required to implement Service, which may include rack space, power, cooling, network connectivity, public cloud access, or other modifications | R, A | I |
| | Send CTA(s) to Customer-provided location(s) (if using physical CTAs) | I | R, A |
| **Service Implementation** | Provide Secureworks with access (e.g., login credentials, access to Customer network) to Devices that Secureworks will manage | R, A | I |
| | Implement all requirements per guidelines provided to Customer by Secureworks | R, A | I |
| | Install the CTA(s), and use cables to appropriately connect the CTA(s) to the network<br>***Note:*** In Japan, Customer and Secureworks can agree to on-site installation and device provisioning per a SOW as applicable. | R, A | I |
| | Finish configuration of CTA(s) (remotely) | I | R, A |
| | Configure implementation rules on Customer | R, A | I |

| AETD Carbon Black Response Cloud | | | |
|---|---|---|---|
| **Activity** | **Task** | **Customer** | **Secureworks** |
| | side based on guidelines provided by Secureworks, third-party vendor, or both, as applicable | | |
| | Configure implementation rules in the Secureworks environment | I | R, A |
| | Configure Endpoints (e.g., hosts, laptops) for Security Event logging | R, A | I |
| | Configure Secureworks Client Portal and Carbon Black Cloud Response Cloud access for Customer's authorized users | I | R, A |
| | Provide training (remotely) to Customer for Secureworks Client Portal | I | R, A |
| | Provide Customer-side post-install validation steps to Customer | I | R, A |
| | Complete Customer-side post-install validation steps | R, A | I |
| | Complete Secureworks-side post-install validation steps | I | R, A |
| **Security Monitoring** | Conduct daily monitoring activities to include review, triage, and forwarding of Customer-related validated alerts/Security Events/Security Incidents for next steps | I | R, A |
| | Conduct incident response activities for alerts, Security Events or Security Incidents identified by Secureworks | R, A | I |
| | Monitor Service-specific logs and create Security Events or Security Incidents for security concerns | C, I | R, A |
| | Conduct real-time analysis of Security Events that are created (manually create Security Incident tickets if needed); escalate Security Incidents as applicable, using Customer's escalation procedures | C, I | R, A |
| | Conduct log correlation to identify internal sources/destinations of traffic related to escalated Security Incidents (if applicable) | I | R, A |

| AETD Carbon Black Response Cloud | | | |
|---|---|---|---|
| **Activity** | **Task** | **Customer** | **Secureworks** |
| | Submit ticket through Secureworks Client Portal to request Security Event tuning calls (include sample of events or incidents) at least five (5) days in advance; Secureworks will provide Customer with guidance | R, A | I |
| | Adjust filters, MPLE rules, and escalation criteria to meet Customer's incident alerting requirements as a result of Security Event tuning calls | I | R, A |
| | Submit through Secureworks Client Portal (or otherwise contact SOC to submit) request to create custom IP watch lists and related alerting procedures (submit changes to watch lists and alerting procedures through Portal as needed) | R, A | C, I |
| | Implement Customer-provided custom IP watch lists and related alerting procedures (update as needed, upon request from Customer) | C, I | R, A |
| | Remediate all malware and threat actor activity | R, A | I |
| **Change Management** | Investigate and confirm validity and potential business impacts of changes (i.e., conduct due diligence) prior to submitting any change request in Secureworks Client Portal for implementation, such as changes to policies, process disruption, hash banning, or Endpoint isolation | R, A | I |
| | Submit through Secureworks Client Portal (or otherwise contact SOC to submit) all change requests for Devices; ensure requests are internally vetted and approved within Customer's organization, and include all information necessary to implement each request | R, A | I |
| | Advise Secureworks of appropriate timing for maintenance window to perform changes (e.g., Customer-submitted change requests) and maintenance (e.g., in-scope software upgrades) for Devices | R, A | C, I |
| | Perform maintenance that is specific to Customer's environment and implement Customer-submitted change requests during | C, I | R, A |

| AETD Carbon Black Response Cloud | | | |
|---|---|---|---|
| **Activity** | **Task** | **Customer** | **Secureworks** |
| | the Customer-designated maintenance window | | |
| | Perform validation on completed changes to Devices in Customer's environment | R, A | C |
| | Notify Customer (through Secureworks Client Portal or email) that requested change was completed | I | R, A |
| | Provide explicit approval for Secureworks to implement emergency IP blocks without first obtaining Customer approval (optional) | R, A | C, I |
| | Implement emergency blocking-rule changes as necessary (e.g., to address real-time malicious traffic) | C, I | R, A |
| | Advise Customer of emergency blocking-rule changes after implementation | C, I | R, A |
| | Notify Secureworks through Secureworks Client Portal or telephone of issues that occur after changes have been implemented | R, A | I |
| | Investigate Customer-reported issue(s) with changes made, and revert to previous state if Secureworks-implemented changes caused issue(s) | A, C | R |
| | Conduct ad-hoc changes and troubleshooting that is out of scope for the Service | R, A | I |
| **Support** | Conduct troubleshooting related to the Service to determine root cause of an issue | C, I | R, A |
| | Support validation (including validation for health-related issue) for upgrades and updates implemented on Endpoints | I | R, A |
| | Contact vendor for assistance with Endpoint Sensor Software troubleshooting | R, A | C, I |
| | Conduct software upgrades and configuration changes that are in scope for the Service *(software must be Secureworks supported)* | C, I | R, A |
| | Provide on-site personnel to assist Secureworks while conducting any activity that must be physically performed on-site | R, A | C, I |

| AETD Carbon Black Response Cloud | | | |
|---|---|---|---|
| **Activity** | **Task** | **Customer** | **Secureworks** |
| | Send electronic notification to Customer about critical Device vulnerabilities and requests for authorization to apply a patch or patches (if applicable to one or more Devices) | C, I | R, A |
| | Provide support to Customer for issues relating to the Secureworks Client Portal (including mobile access) and Carbon Black Response Cloud | C, I | R, A |
| | Ensure Secureworks has current contact information for authorized contacts regarding Customer's account | R, A | I |
| **General** | Provide Secureworks with advance notice of Customer-authorized scans or Customer network maintenance periods (to avoid unnecessary Secureworks escalations resulting from these activities) | R, A | I |
| | Provide Customer network design and specification for integration with Secureworks services (includes auditing and providing updated designs and specifications when changes are made) | R, A | I |
| | Download and register mobile application (named "Secureworks Mobile") to mobile device from an application store | R, A | C |
| | Maintain network ranges (e.g., public, DMZ, and private) and network translation devices (e.g., NAT pools, proxies, and load balancers) | R, A | C, I |
| | Notify Secureworks of any changes to network ranges (e.g., public, DMZ, and private) and changes to network translation devices (e.g., NAT pools, proxies, and load balancers) | R, A | C, I |
| | Maintain valid vendor support contracts for all monitored Endpoints | R, A | I |
| | Update Endpoint Sensor software when notified that updates are available from endpoint sensor vendor | R, A | I |
| | Update Endpoint Sensor software | R, A | I |

### 2.3.6 Secureworks Platform Maintenance

To ensure Customer receives the highest level of Service possible, Secureworks will conduct platform maintenance (updates, upgrades, patching, and other platform-specific work) on a periodic basis, as maintenance changes are validated and approved for release into the Secureworks platform. Secureworks follows internal change control processes to ensure platform stability. Generally, maintenance does not require a network outage. Secureworks will conduct platform maintenance without Customer approval or a maintenance window when a network outage is not required. Customer acknowledges and agrees that approval or a maintenance window is only mandatory when a network outage is required.

## 2.4 Training and Documentation

Each new Secureworks Customer can participate in foundational training for Secureworks Managed Security Services Integration. Foundational training (primarily webinar-based) is offered to align and mature Customer's Secureworks Managed Security Services Integration and compliment the service implementation process. The training is scheduled during the service implementation process, and is delivered through live, interactive training sessions. Other Service-specific training may be provided. Foundational training includes the following topics, as applicable to the Service:

- Portal Training
- Portal User Roles and Audit
- Escalation Procedures
- MPLE Rules Review
- Ticket Review and Baseline Portal Reports
- Managed Device Alignment (e.g., ensuring understanding of expectations between Customer and Secureworks regarding Devices being managed by Secureworks)

Customer is responsible for its own training and documentation for any third-party products used as part of the Service.

Secureworks will provide Service-related documentation to Customer. Documentation is generally provided through the Secureworks Client Portal.

## 2.5 Support for Private Virtual Environments

Depending on Device types, Customer's environment, Customer's requirements, and other criteria, Secureworks provides support as described herein, for a single-tenant Private Virtual Environment that is located on Customer's premises as part of a service that Customer purchases from Secureworks. The information in this section is part of Customer agreement with Secureworks, and takes precedence over any conflicting information elsewhere in this SD. The subsections below contain information about Customer responsibilities, Secureworks responsibilities, and out-of-scope services with regard to a Customer's Private Virtual Environment. See the Glossary for definitions of terms related to virtualization that are used in this SD.

### 2.5.1 Customer Responsibilities

Customer agrees to the responsibilities explained in the subsections below and acknowledges and agrees that Secureworks' ability to perform its obligations and responsibilities, and its liability under the SLAs, are dependent upon Customer's compliance with these responsibilities.

#### 2.5.1.1 Provisioning and Maintenance

Customer is responsible for all aspects of provisioning (installation, configuration, and setup) of supported Hypervisor technology, such as VMware, including but not limited to the following:

- Virtual switches
- Virtual network interfaces
- Virtual networks
- VMs

Customer must perform all maintenance for the Guest VM, which includes the items listed below.

- Guest VM snapshot backup
- Restoration of the image on the Guest VM
- Underlying Hypervisor that provides in-band management access (e.g., access to the Customer's network through Simple Network Management Protocol/SNMP) for Secureworks (*Customer must resolve in-band access issues in case of loss of network connectivity for Secureworks to manage the vCTA and if applicable, Virtual Security Appliance*)
- Troubleshooting (Hypervisor, hardware, and Host/Guest VM)

#### 2.5.1.2 VMs

Customer is responsible for providing the Guest VM(s) on which the Secureworks-provided image (the vCTA) and, if applicable, Virtual Security Appliance ("VSA") will be installed. Customer must provision the VM with the required central processing unit ("CPU"), memory, storage capacity, and network resources needed for proper functionality and delivery of the Service. Customer shall provide Secureworks with a privileged account with access to the Guest VM(s). This account may also be used for automation purposes. The OS on the Guest VM must have a valid license for support. Secureworks will not provide any assistance without in-band access to the Guest VM and without a valid license.

### 2.5.2 Secureworks Responsibilities

Secureworks is responsible for providing the vCTA and, if applicable, VSA, providing support to Customer during provisioning of the vCTA and VSA, and managing and monitoring the vCTA and VSA that are operating on the Guest VM(s). Customer must maintain a suitable environment in which to operate the Guest VM(s) that is being used for the vCTA and VSA. This includes using a Secureworks-supported Hypervisor version.

### 2.5.3 Shared Responsibilities

#### 2.5.3.1 VSA and vCTA Upgrades

Secureworks will implement upgrades only for the VSA and vCTA on the Guest VM, as applicable to the Service; Customer is responsible for any other upgrades (e.g., Host/Guest VM, Hypervisor).

#### 2.5.3.2 VSA and vCTA Backups

Secureworks will back up the configuration for the VSA and vCTA only. It is Customer's responsibility to back up (and otherwise maintain) the image or virtual hard disk for the Guest VM. If a Guest VM requires a rebuild, then Secureworks will restore the prior vCTA configuration after Customer restores the Guest VM and its connectivity. Secureworks recommends that any virtual infrastructure be deployed on redundant systems.

### 2.5.4 VSA and vCTA Health, and Adding Capacity

Secureworks will perform health-related validations on the VSA. Secureworks must be able to connect to the VSA through the Internet using ICMP and SSH. Each VSA is always assumed to be powered on, and any disappearance of a VSA from the network is considered a failure.

Secureworks will monitor the vCTA. If it is determined that a health-related issue caused by performance of the Host/Guest VM hardware, or insufficient capacity for the Guest VM, is negatively affecting the vCTA, then it is Customer's responsibility to resolve the performance issue or add sufficient capacity to the Guest VM.

Secureworks will perform availability monitoring of the VSA and vCTA using periodic polling of (approximately every 1-5 minutes; timing is subject to change) of each Device. If a failed or negative response is received through polling, then an automatic alert is sent to Secureworks, which then generates a ticket. Secureworks will conduct troubleshooting and contact Customer as applicable to the Service.

Health monitoring is limited to VSAs, CTAs, and other Devices. Secureworks does not perform health monitoring for Hypervisors or underlying hardware.

### 2.5.5 Out-of-Scope Services in a Virtual Environment

The following are considered out-of-scope for this Service:

- Restoring the VM image backups
- Troubleshooting issues at the Hypervisor level
- Troubleshooting performance issues not directly related to the VSA or the vCTA (i.e., the image on the Guest VM) such as hardware, Hypervisor, or Host-level issues
- Anything not specifically described herein as part of the standard offering for the Service

## 2.6 Out of Scope

The information in Section 2 comprises the Secureworks standard in-scope offering for the Service. Any other services or activities not specifically listed as in scope are out of scope. Items listed below are examples of services and activities that are out of scope. Upon request, Secureworks can provide out-of-scope technical support on a time and materials basis pursuant to a separate SO or Statement of Work ("**SOW**").

- Custom reports and customizing AETD-generated reports
- Dedicated incident response services
- Installation and provisioning of Endpoint Sensors
- Analysis of minor events
- Integration of complementary products that are not managed by Secureworks (e.g., anti-virus software, web reporting software)
- Vendor API Integration
- Remediation of malware and threat actor activity
- Training on the Carbon Black Response Cloud

# 3 Service Fees and Related Information

Service Fees are based on the number of licenses Customer purchased for Carbon Black Response Cloud. See Customer's MSA or CRA (as applicable), and SO or SOW (as applicable) for details, including the following:

- Billing and Invoicing
- Out-of-Pocket Expenses
- Services Term

### 3.1 Invoice Commencement

See the Service-specific Addendum or SO for information about invoice commencement.

## 4 Recommended Add-on Services

The Secureworks offerings listed below are optional and are sold independent of this Service or bundled with this Service. In addition, output from the Service can be used in delivering these add-on Services for an additional charge.

- **Managed Security Services**
  - **Global Threat Intelligence ("TI"):** Secureworks will make available to Customer through the Secureworks Client Portal a collection of threat intelligence (i.e., reports, data feeds, and related content and information about any technique or software used to exploit vulnerabilities) that will help Customer to understand the threat landscape, protect against cyber threats and vulnerabilities, and mitigate risk in its environment. The TI provides Customer with analysis of emerging threats and vulnerabilities, and deliver early warnings and actionable global TI. A monthly TI webinar that Secureworks hosts will be available to Customer.
- **Professional Services**
  - **Incident Management Retainer ("IMR"):** Secureworks will provide Customer with emergency and/or proactive incident response services such as incident response readiness, planning, workshops, and related services; digital forensic analysis; and threat hunting.

## 5 Service Level Agreements ("SLAs")

The table below contains the SLAs that are applicable to the Service.

| SLA | Description | Credit |
|---|---|---|
| Security Monitoring *(Security Incident Analysis)* | Customer shall receive electronic notification of a Security Incident in accordance with Customer's defined escalation procedures within fifteen (15) minutes of the determination by Secureworks that the given activity constitutes a Security Incident. This is measured by the difference between the time stamp on the incident ticket created by Secureworks SOC personnel or technology and the time stamp of the correspondence documenting the initial escalation.<br>Security incidents generated from long-term correlation logic and retroactive analyses based on newly identified threat indicators are not subject to this SLA.<br>Event(s) deemed low severity may be sent to Customer for review, and will be available through the Portal for reporting. | 1/30th of monthly fee for Service for the affected Device |
| Incident Investigations *(AETD Carbon Black* | Upon generation of an AETD Carbon Black Response Cloud-based Security Incident designated by Secureworks as significant, Secureworks will provide an Incident Investigation | 1/30th of monthly fee for Service for the affected |

| SLA | Description | Credit |
|---|---|---|
| *Response Cloud and Red Cloak)* | within twenty-four (24) hours from the timestamp of creation of the Security Incident.<br>Requests for Incident Investigations that Secureworks does not deem significant are performed at the discretion of Secureworks and with no associated SLAs. Some requests may be referred to professional services through a separately signed Statement of Work. | Device |
| Service Request | A service request (applies to all non-change and non-incident tickets) submitted through telephone or the Secureworks Client Portal will be acknowledged through human or electronic notification (e.g., Portal, mobile app) within one (1) hour from the creation time stamp on the ticket.<br>Customer must contact SOC through telephone or the Chat in the Portal for immediate engagement with urgent service request tickets. | 1/30th of monthly fee for Service for each calendar day the service request was not acknowledged within the specified timeframe |
| Availability | Communications availability to the Internet and Customer access to the Portal shall equal no less than 99.9% of the time during any calendar month.<br>“Communications availability” is defined as the ability of a Secureworks SOC to successfully send and receive TCP/IP packets between the CTP and its upstream Internet service provider.<br>“Customer access to the Portal” is defined as the ability of the Secureworks monitoring service to successfully log in to the Portal.<br>Secureworks does not provide a guarantee with regard to availability or performance of the Internet. Measurement of 99.9% is executed from multiple sites connecting to a Secureworks SOC. | 1/30th of monthly fee for Service each day in which the Service fails to meet this SLA |

**Warranty Exclusion:** While the Service is intended to reduce risk, it is impossible to completely eliminate risk, and therefore Secureworks makes no guarantee that intrusion, compromises, or any other unauthorized activity will not occur on Customer’s network.

The SLAs set forth above are subject to the following limitations:

- Secureworks schedules maintenance outages for Secureworks-owned equipment that is being used to provide the Service and will provide Customer-designated contact(s) with 24 hours of notice of an outage. The SLAs shall not apply during scheduled maintenance outages, and no SLA credit shall apply during a maintenance outage.
- Secureworks shall not be responsible for any Service impact related to any product configuration on a managed Device that is not supported by Secureworks.
- The SLAs shall not apply if any act or omission by Customer prohibits or otherwise limits Secureworks from providing the Service or meeting the SLAs, including but not limited to misconduct, negligence, provision of inaccurate or incomplete information, modifications to the

Service, or any unauthorized modifications made to any managed hardware or software Devices, by Customer or its employees, or third parties acting on behalf of Customer.

- The SLAs shall not apply to the extent Customer does not fulfill and comply with the obligations and responsibilities set forth within this SD. The obligations of Secureworks to comply with the SLAs with respect to any Security Incident response or Service Request are also dependent on Secureworks' ability to connect directly to Customer-Side Technology on Customer's network.
- The SLAs shall not apply if Customer-Side Technology is unreachable due to network connectivity issues, authentication issues, configuration issues, or public cloud downtimes that are outside the direct control of Secureworks.

For Customer to receive an SLA credit, subject to the limitations above, the notification of the SLA failure must be submitted to Secureworks within thirty (30) days of the date of such SLA failure. Secureworks will research the notification and respond to Customer within thirty (30) days from the date such notification is received. The total amount credited to Customer in connection with any of the above SLAs in any calendar month will not exceed the monthly Service fees paid by Customer for such Service. The foregoing SLA credit(s) shall be Customer's sole and exclusive remedy for failure to meet or exceed the foregoing SLAs.

# 6 Additional Considerations and Information

## 6.1 Secureworks-Provided Licenses

If Customer purchases AETD licensing from Secureworks, then Secureworks will:

- Procure the license(s)
- Configure the license(s)
- Troubleshoot and remediate all license issues
- Facilitate renewal of the license (for an additional charge)

## 6.2 Secureworks Lifecycle Policy and Related Information

Secureworks provides its Lifecycle Policy through this link: https://www.secureworks.com/client-support/lifecycle-policy. This policy includes information for customers purchasing service bundles and products. Use the following link for direct access to the Policy ***in PDF format***: Secureworks Lifecycle Policy. Customer can also access the Secureworks Hardware and Software Support Status matrix, End-of-Sale ("**EOS**") and End-of-Life ("**EOL**") notifications, and other information through the aforementioned link. Secureworks reserves the right to alter the General Availability ("**GA**"), EOS, and EOL dates at any time for any reason. Secureworks is not responsible for errors within the Hardware and Software Support Status matrix.

## 6.3 Carbon Black Response Cloud Endpoint Sensor Software Installation, Management, Maintenance, and Limitation of Liability

1) The installation, ongoing management, and maintenance of Endpoint Sensor software are the sole responsibility of Customer.
2) Customer can install and perform ongoing management of the Endpoint Sensor software by utilizing the Carbon Black Management Console and the Carbon Black Response Cloud user guide in combination with Customer's software distribution process.
3) SECUREWORKS WILL NOT BE RESPONSIBLE FOR ANY LOSSES, COSTS, OR DAMAGES RELATING TO THE INSTALLATION OF THE ENDPOINT USER SOFTWARE. SECUREWORKS

STRONGLY RECOMMENDS THAT THE CUSTOMER INSTALL AND EVALUATE ENDPOINT SENSOR SOFTWARE IN A TEST ENVIRONMENT AND DEPLOY IT IN SMALL BATCHES IN ACCORDANCE WITH CUSTOMER'S CHANGE MANAGEMENT POLICIES TO ENSURE THERE ARE NO ISSUES BEFORE IMPLEMENTING IT AS TO ITS ENTIRE INFRASTRUCTURE.

4) SECUREWORKS WILL NOT BE RESPONSIBLE FOR ANY IMPACT THAT MAY BE INCURRED FROM INSTALLING ENDPOINT SENSOR SOFTWARE ON AN UNSUPPORTED OPERATING SYSTEM OR CUSTOM BUILT IMAGE.

5) SECUREWORKS WILL NOT BE RESPONSIBLE FOR ANY IMPACT FROM CUSTOMER'S FAILURE TO COMPLY WITH THE ENDPOINT SENSOR SOFTWARE UPDATING PROCESS.

6) SECUREWORKS WILL NOT BE RESPONSIBLE FOR ANY LOSSES, COSTS, OR DAMAGES RELATING TO THE INSTALLATION OF THE END POINT USER SOFTWARE ON ANY ENDPOINTS NOT OWNED BY CUSTOMER.

7) THE SOFTWARE MAY COME BUNDLED OR OTHERWISE BE DISTRIBUTED WITH OPEN SOURCE OR OTHER THIRD PARTY SOFTWARE, WHICH IS SUBJECT TO THE TERMS AND CONDITIONS OF THE SPECIFIC LICENSE UNDER WHICH IT IS DISTRIBUTED. OPEN SOURCE SOFTWARE IS PROVIDED BY SECUREWORKS "AS IS" WITHOUT ANY WARRANTY, EXPRESS, IMPLIED, OR OTHERWISE, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. SECUREWORKS SHALL HAVE NO RESPONSIBILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF OPEN SOURCE SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. UNDER CERTAIN OPEN SOURCE SOFTWARE LICENSES, YOU ARE ENTITLED TO OBTAIN THE CORRESPONDING SOURCE FILES. YOU MAY FIND CORRESPONDING SOURCE FILES FOR THE SOFTWARE IN THE CARBON BLACK MANAGEMENT CONSOLE.

### 6.3.1 Endpoint Sensor Count and Contract Alignment

1) It is Customer's responsibility to ensure the contracted amount of Endpoints is not exceeded.

2) If at any time throughout the course of the Agreement, Secureworks determines that Customer's total number of Endpoints exceeds the number of Eendpoints contracted for, a change order will be required. The change order will reflect both the change in number of Endpoints, and the corresponding increase in charges. Customer hereby agrees to a change order and pays for any corresponding increase in charges (when applicable).

### 6.3.2 Contract Termination and Endpoint Sensor Software Removal

Secureworks will decommission all Customer domain(s) immediately upon the termination date or end date of the Agreement. Once a contract is terminated it is Customer's responsibility to remove all Endpoint Sensor software from its environment by the termination date. SECUREWORKS WILL NOT BE RESPONSIBLE FOR ANY LOSSES, DAMAGES, OR COSTS RELATING TO CUSTOMER'S FAILURE TO REMOVE ALL ENDPOINT SENSOR SOFTWARE FROM ITS ENVIRONMENT AS OF THE TERMINATION DATE.

## 7 Glossary

| Term | Description |
|---|---|
| Counter Threat | Equipment that specifically allows Secureworks to collect data while |

| Term | Description |
|---|---|
| Appliance (“**CTA**”) | performing a Secureworks-defined service for Customer, such as monitoring Customer’s network and environment for security threats. |
| Counter Threat Platform ("**CTP**") | A Secureworks proprietary MSS Services platform that ingests log data to produce events within the platform, which are then correlated and analyzed to protect Customer’s organization from emerging and existing threats. |
| Counter Threat Unit (“**CTU**”) | Internal team of security experts that research and analyze threat data across Secureworks global Customer base and actively monitors the threat landscape. Provides threat intelligence that extends visibility into cyber threats beyond the edges of the networks of Secureworks Customers. The threat intelligence, applied to technology and the Secureworks suite of services, enables Customers to expand visibility and reduce the time it takes to see and respond to them, thereby resisting and avoiding cyberattacks. |
| Customer Device(s) | One or more Devices that are owned by Customer and were not purchased from Secureworks. |
| Due Diligence | Validating the accuracy of information used to create Customer's original Service Order against the actual environment in which services will be performed. |
| Endpoint | An Internet-capable computing machine or end unit such as a desktop computer, laptop, smart phone, tablet, thin client, or another similar device. |
| Endpoint Sensor Software | Software installed on an Endpoint for sending telemetry to the application that is enabling monitoring of the Endpoint. |
| Event Flow Disruption ("**EFD**") | A proactive method that detects differences with logs being sent to Secureworks from individual Devices – e.g., complete loss of log flow, incorrect log format, or an overall lack of logs to trigger Security Event generation within the CTP. |
| General Availability ("**GA**") | The date on which hardware or software is made available to the public for purchase. |
| Identified Changes | Differences (e.g., Device quantity, make, model, software package, or software version) that are discovered while conducting due diligence for the Service. |
| In-Band | Activity within a defined telecommunications frequency band. |
| Multi-Purpose Logic Engine ("**MPLE**") | Secureworks proprietary tool that uses specific rules to identify, in real time, patterns that may indicate malicious activity. |
| Private Virtual Environment | Customer’s on-premises virtual infrastructure. |
| Public Cloud Environment | Third-party virtual infrastructure that hosts Customer’s network and security devices. |

| Term | Description |
|---|---|
| Security Event | Identified occurrence of a system or network state that may be malicious, anomalous, or informational, which is ingested into the Secureworks technology infrastructure. |
| Security Incident | One or more related and identified Security Events that can potentially impact the confidentiality, integrity, or availability of a Customer's information or systems, and requires further analysis and disposition. |
| Service Level Agreement ("**SLA**") | One or more related and identified Security Events that can potentially impact the confidentiality, integrity, or availability of a Customer's information or systems, and requires further analysis and disposition. |
| **Definitions for Virtual Environments** | |
| Guest | Separate and independent instance of operating system and application software that operates on a Host. |
| Host | Virtual Machine host server that provides the physical computing resources, such as processing power, memory, disk, and network I/O. |
| Hypervisor | Virtual Machine monitor that isolates each Guest, enabling multiple Guests to reside and operate on the Host simultaneously. |
| Virtual Contexts | A form of virtualization where one physical firewall is divided into two (2) or more virtual firewalls. |
| Virtual Machine (“**VM**”) | A logical instance of the physical Host that houses the operating system of the Guest. |
| Virtual Security Appliance (“**VSA**”) | Software implementation of a security device—e.g., a log retention appliance, scanner appliance (VMS), intrusion detection system—that executes programs in the same manner as a physical machine. |