Secureworks®

SERVICE DESCRIPTION

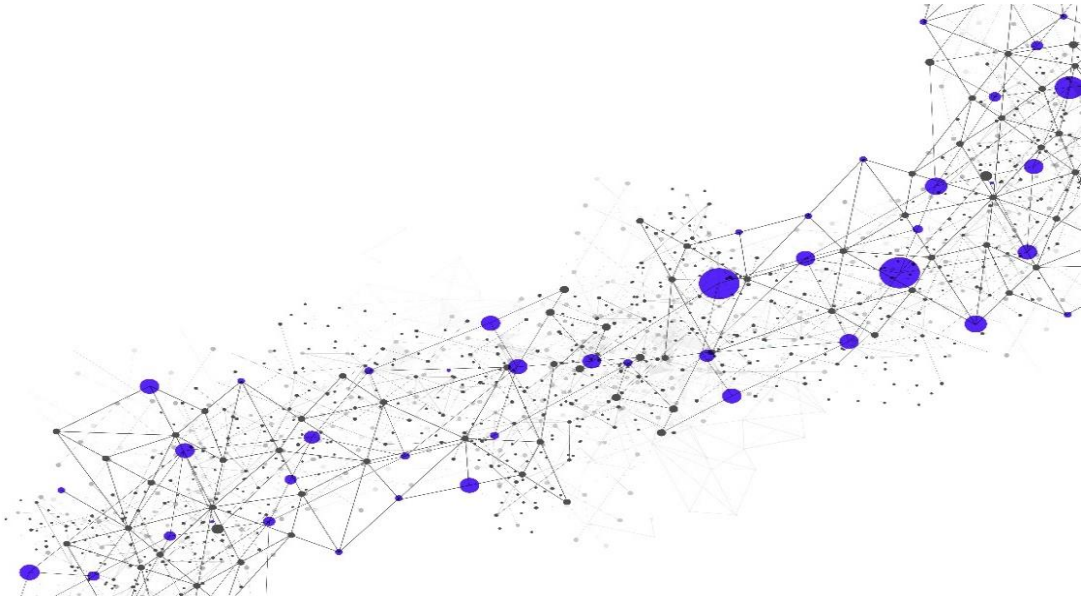
Advanced Endpoint Threat Detection (AETD) with CrowdStrike or AETD Elite with CrowdStrike

Release Date

May 14, 2021

Version

25.1



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

1 Service Introduction

This Service Description ("**SD**") describes both the Advanced Endpoint Threat Detection ("**AETD**") with CrowdStrike and the AETD Elite with CrowdStrike 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., MPLE tuning, Red Cloak™ watchlist and suppression rule modifications), and rule/policy modifications; CrowdStrike watchlist tuning is not included
- Monitoring and alerting to detect event data (log) flow issues for the Service
- Managing the Secureworks Red Cloak hosted infrastructure

1.1 Overview

The Service consists of monitoring Endpoints operating on systems that are compatible with the CrowdStrike Agent (also referred to as "**Agent**" or "**Device**" in this SD) to detect signs of advanced threats and threat actors, search for specific indicators of compromise, maintain updated threat intelligence ("**TI**"), analyze telemetry, and send alerts to Customer with recommendations on how to proceed should threat activity be detected. To perform these activities, Customer installs Agents on Customer's Endpoints, and the Agents send event data that is processed through Secureworks Red Cloak Analytics (which contains Secureworks TI), and is then processed 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.

In addition, 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.

Each Endpoint must be licensed for use of one CrowdStrike Agent (and one Red Cloak Inspector™ Module if Customer purchases AETD Elite) for monitoring and alerting Customer of suspicious activity on the Endpoint. Customer will procure the appropriate number of AETD licenses for the CrowdStrike Agents from Secureworks or Partner, and if applicable, will procure the appropriate number of licenses for Red Cloak Inspector Modules from Secureworks.

The table below indicates the components of the two options for the Service.

AETD with CrowdStrike	AETD Elite with CrowdStrike (*see Appendix*)
• Security Event Monitoring and Alerting (including additional analysis and investigation for Security Incidents that Secureworks deems critical) • Event Flow Monitoring and Alerting • Data Flow Integration (between CTP and CrowdStrike Falcon) • Management Activities	All components of AETD with CrowdStrike ***plus –*** • Active Threat Hunting as follows: • Review of evidence and artifacts present on Customer's Endpoints and in other Customer Data to identify threats and threat actors • Weekly Threat Hunting Summary Reports • Weekly Touchpoint Meetings

Notes:

- If ***AETD Elite*** is purchased, then Active Threat Hunting ("**ATH**") is included as an add-on component of the Service. See the Appendix in this SD for details.
- **A Falcon Insight license is required for CrowdStrike to enable event flow through the Falcon Data Replicator**. Customer can purchase this license from Secureworks or CrowdStrike. Customer must have CrowdStrike Falcon Insight (for Endpoint Detection and Response) for the CTP to receive any telemetry from CrowdStrike Falcon Prevent (Next Generation Antivirus - NGAV). Falcon Insight gathers the telemetry that is sent to the CTP. Customer can purchase the license for Falcon Insight from Secureworks or CrowdStrike.

  Falcon Prevent (NGAV) is only an alert provider; therefore, if Customer only has CrowdStrike Falcon Prevent (NGAV), then the CTP will not receive any telemetry from it.

See Section 2, Service Details, for more information about the Service, including further explanation of the components listed above. Also, see the **Secureworks MSS Services – Service Description Addendum** for information about the following, as applicable to the Service: Device responsibilities, Maintenance Program, and Subscription Program.

Note: Secureworks will not install or update 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 Management for Agents and Inspector Modules

1.2.1.1 CrowdStrike Agent

Customer will manage and troubleshoot the CrowdStrike Agents that are installed on Endpoints including the following:

- All troubleshooting of CrowdStrike Agent (including contacting Partner for assistance)
- Monitoring CrowdStrike Agent availability and performance through the CrowdStrike Management Console
- Customer will contact SOC to request assistance with CrowdStrike host isolation or process disruption. Customer will manage prevention hashes and Endpoint threat prevention policies.

1.2.1.2 Red Cloak Inspector Modules (for AETD Elite only)

If Customer purchases AETD Elite, then Customer will manage and troubleshoot the Red Cloak Inspector Modules that are installed on Endpoints including the following:

- Contacting Secureworks for assistance with troubleshooting
- Monitoring Red Cloak Inspector Module availability and performance through the Red Cloak Portal

1.2.1.3 General (for both CrowdStrike Agents and Red Cloak Inspector Modules)

Customer will do the following:

- Ensure all operating systems ("OSs") for the CrowdStrike Agents that are in scope for the Service are supported by CrowdStrike; if AETD Elite is purchased, then also ensure that the OSs are supported by Secureworks

- Ensure Endpoints have sufficient available resources for installation and operation of the Agents (and Red Cloak Inspector Modules if applicable) as defined by CrowdStrike and Secureworks operating environment requirements
- Install the Agents (and Red Cloak Inspector Modules if applicable) on each Endpoint, and only on Endpoints owned by Customer as Secureworks will deliver the Services only to such Endpoints
- Update/upgrade Agents (and Red Cloak Inspector Modules if applicable) as needed; use a process to deploy updates/upgrades first in a test environment, and assess any impact before deploying updates to production Endpoints and environments
- Ensure availability of the Agents (and Red Cloak Inspector Modules if applicable)
- Respond to and remediate issues with Agent (and Red Cloak Inspector Modules if applicable) availability and performance
- Conduct all required ongoing maintenance of the Agents (and Red Cloak Inspector Modules if applicable)
- Reinstall Agents (and Red Cloak Inspector Modules if applicable) as required
- Remove all Agents (and Red Cloak Inspector Modules if applicable) from all Endpoints and Customer's environment by the contract end or termination date

1.2.2 Support Contracts and Licensing

Customer acknowledges and agrees that unless Customer has executed an agreement directly with CrowdStrike, Customer's use of the CrowdStrike license is subject to the terms and conditions set forth at https://www.crowdstrike.com/wp-content/uploads/direct/terms-conditions-direct.html.

1.2.3 Connectivity

Customer will provide and maintain remote network connectivity to Customer's environment, including ensuring sufficient network bandwidth, and the in-scope Agents that are necessary for Secureworks to perform the Service. Customer will allow connectivity from Customer locations to CrowdStrike Falcon. If Customer purchases AETD Elite with CrowdStrike, then Customer will also allow connectivity between Secureworks IP ranges and Customer location(s) as applicable to the Service. SLAs will not apply to the Agents that are experiencing connectivity issues that are beyond the control of Secureworks.

1.2.4 Application Program Interface ("API") Integration

Some vendors/Partners 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.

1.2.5 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 Secureworks Client Portal. Customer will communicate with CrowdStrike for CrowdStrike-specific issues.

1.2.6 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.

1.2.7 Usage Overage

If, for any services identified in Customer's Transaction Document(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.

1.2.8 Software Procurement

Customer will license the software necessary for Secureworks to deliver the Service. Customer will ensure that its operating systems 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/Partner or supported by Secureworks.

1.2.9 Licenses and Support Contract for CrowdStrike

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

1.2.10 General

Customer will do the following:

- Ensure that Customer personnel are scheduled and available to assist as required for the Service
- Obtain 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
- Provide to Secureworks all required information (key personnel contact information, credentials, and related information) prior to work being started
- Promptly reply to all requests from Secureworks
- Ensure Customer-scheduled downtime and maintenance windows will allow adequate time for Secureworks to perform the Service(s)
- 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)
- Remediate all malware and threat actor activity (unless otherwise contracted with Secureworks under a separate Transaction Document)
- Implement and maintain password policies for external and internal applications (Secureworks recommends Customer implement and maintain password policies that adhere to Section 5, Authenticator and Verifier Requirements, within NIST Special Publication 800-63B)

- Ensure all Endpoints report into CrowdStrike Falcon (and Red Cloak Portal if applicable) at least every 30 days
  - Any Endpoint that has not communicated properly every 30 days will no longer be monitored and will not be included in other analytics or in the total Endpoint count as set forth in Section 6.4
- Manage file lists for applying process disruption in CrowdStrike Falcon (for CrowdStrike Agents)

1.3 Initial Implementation Scheduling and Points of Contact

Secureworks will contact Customer within seven (7) Business Days after execution of the Transaction Document to schedule the first meeting during which Service Implementation will be discussed.

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), 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 Statement of Work ("**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 (see the ***Note*** below), 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 HCTA may be required for a location that was not originally determined to be in scope.

Note: Secureworks will enable Customer's access to the Secureworks Client Portal. If Customer purchases AETD Elite with CrowdStrike, then Secureworks will also enable Customer's access to the Red Cloak Portal. CrowdStrike will enable Customer's access to the CrowdStrike Falcon Portal.

- **Prepare:** Baseline the project schedule, identify required training, and configure HCTAs; Customer provides information necessary to execute implementation for MSS Services
  - For this Service, one or more HCTAs will need to be installed. The HCTA is a Secureworks-proprietary Device that is used in the secure delivery of the Service for Device health and Security Event collection and transport. Secureworks must use one or more **HCTAs deployed in a Secureworks data center or Public Cloud Environment** to communicate with Devices that Secureworks is monitoring for this Service. 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 this requirement.
- **Execute:** Complete configuration of HCTAs and related service-enabling technology, validate ingestion of identified log source(s) if applicable, schedule and deliver foundational training, and activate services

  Notes:

  - Secureworks provides telephone support to Customer for installing Equipment (i.e., Devices Customer purchases or leases from Secureworks).
  - After Equipment is installed, Secureworks will access 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 Secureworks Client 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 (See tasks in the "Service Preparation" portion of RACI in Section 2.3.5, Customer and Secureworks Responsibilities). **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 Equipment is part of the Service, then installation activities are also part of provisioning.

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

- Create implementation ticket in Secureworks Client 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 and Red Cloak Portal
- Collect Customer information that is necessary for implementation
- Complete provisioning and installation activities (e.g., confirming event flow from Devices, configuring Devices within 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
    - 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

2.2 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 through use of the CrowdStrike Agents (and Red Cloak Inspector Modules, if applicable), 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 the Secureworks Counter Threat Unit™ ("**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 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

Red Cloak Analytics uses a combination of Secureworks and third-party derived TI, pattern-based detection, big data analytics, file and process artifact analysis, and threat actor behavior modeling to identify malicious activity on Endpoints. Secureworks will use two methods to identify and act upon Security Incidents, as explained in the table below.

Identification	Description
Real-Time Security Incidents	Upon receiving alerts that are triggered by Endpoint telemetry from CrowdStrike, the alerts are sent to the Secureworks proprietary Multi-Purpose Logic Engine ("**MPLE**") for additional processing and Security Incident creation. Security Events for alerts that are sent to the CTP may be held for 10 to 40 minutes after Secureworks receives them, for correlation and context gathering (actual time depends on the use cases that are 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 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 the sole discretion of Secureworks.

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 that may require immediate attention and/or represent 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 that do not require immediate attention and do not represent a significant threat to a Customer asset – e.g., process-based alerts
Low	Security Events that have little or 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
- 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 CTU 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 rule/policy changes described in this SD 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

Security 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 Event Flow Monitoring and Alerting

Secureworks will use Event Flow Disruption ("**EFD**") to detect data flow issues for the Service (not individual Agents) 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 Partner 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.

2.2.3 Data Flow Integration

Secureworks will integrate CTP with CrowdStrike Falcon. This integration includes configuring CTP to ensure proper data flow from CrowdStrike Falcon to CTP for monitoring and alerting Customer of potential threat actors and threat activity. Customer will be able to view event data from CrowdStrike Falcon in the Secureworks Client Portal.

2.2.4 Management Activities

Secureworks will perform the following management activities:

- Provide a managed, hosted Red Cloak infrastructure with 30 days of data retention (includes software updates, patches, and upgrades)
- Provide guidance on how to access service and product documentation
- Provide provisioning assistance for implementing in-scope services

- Provide the Red Cloak Inspector Module to be downloaded by Customer
- Assist Customer with troubleshooting issues related to the Red Cloak Inspector Module
- Apply TI that is produced by the CTU and Secureworks-selected third-party vendor intelligence sources to Red Cloak Portal infrastructure
- Monitor Endpoint health through the Red Cloak Portal for the hosted Red Cloak infrastructure
- When requested by Customer, provide authorized users with access to the portals
- Display valid Security Events to Customer in the portals
- Display Security Events of interest in the Secureworks Client Portal and Red Cloak Portal
- Use technology combined with a team of security analysts to analyze Endpoint telemetry that is sent to the CTP through Red Cloak Analytics to determine whether an escalation is required and, if so, escalate the incident per Customer's established escalation procedures
- Collect Endpoint telemetry in CTP for potential use with other Services that Secureworks may be providing for Customer
- For threats classified by Secureworks as non-critical, provide alert and automated context information to Customer with available TI attached
- For threats classified by Secureworks as critical, provide alert and automated context information to Customer with available TI attached, and additional investigation information as described in Section 2.2.1.5, Incident Investigations with Red Cloak

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 Secureworks Client 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, Red Cloak Portal, and 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. The Secureworks Client Portal provides access to events and incident tickets, and the Red Cloak Portal provides features and capabilities for Endpoint telemetry and further investigation of threat and threat actor activity. In addition, one or more HCTAs will be provisioned. Below are explanations of these items.

2.3.4.1 Secureworks Client Portal

The Secureworks Client 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, Secureworks Client Portal-specific features, and related content)

Access to the Secureworks Client 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 use of the Secureworks Client Portal is conducted during the Execute phase of service implementation. It is Customer's responsibility to ensure that access for authorized users of the Secureworks Client Portal remains current.

All information received by Customer through the Secureworks Client 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 Red Cloak Portal

The Red Cloak Portal, which contains information about Customer's Endpoint, is the online site for customers with AETD Red Cloak, and provides the following:

- Visibility into AETD Red Cloak functionality and Endpoint-specific information, including events, watchlist results, and other alerts
- Ability to search through retained telemetry from Customer's Endpoints, or visualize the telemetry through custom dashboard widgets
- Ability to create an investigation to organize events related to an incident or attacker activity patterns
- Access to the Secureworks Learning Center (training and self-education – webinars, documentation, SDs, Red Cloak-specific features, and related content)

2.3.4.4 Hosted Counter Threat Appliance ("**HCTA**")

The Service requires one or more HCTAs to communicate with Customer-Side Technology (e.g., for data collection and transfer for monitored Devices). HCTAs will be provisioned in advance of Service Commencement Date and meet minimum hardware and version requirements.

2.3.5 Customer and Secureworks Responsibilities

The following responsibility assignment matrix describes the participation required by both Customer, Secureworks, and Partner in completing tasks or deliverables for a project or business process to facilitate successful service delivery. Secureworks uses the 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. Also, In the RACI table below, use of "Agent" or "Agents" includes the Red Cloak Inspector Module if Customer purchases AETD Elite.

AETD with CrowdStrike or AETD Elite with CrowdStrike				
Activity	**Task**	**Customer**	**Secureworks**	**Partner**
Service Preparation	Provide contact information for authorized contacts regarding Customer's account	R, A	C, I	
	Provide information for authorized users who need access to the Secureworks Client Portal and Red Cloak Portal (Customer will modify as needed at any time through the Secureworks Client Portal, and add / remove users as needed)	R, A	I	
	Create and provide to Secureworks the escalation procedures to follow for tickets (Customer can modify as needed at any time through the Secureworks Client Portal)	R, A	I	
	Enter Customer's initial escalation procedures into Secureworks Client Portal; modify when needed per Customer request	A, C, I	R	
	Provide to Customer the implementation guidelines for service implementation	I	R, A	R, A
	Ensure in-scope Endpoints meet hardware and software specifications of both Secureworks and Partner prior to the start of implementation	R, A	C, I	C, I

AETD with CrowdStrike or AETD Elite with CrowdStrike				
Activity	**Task**	**Customer**	**Secureworks**	**Partner**
Service Implementation	Implement all requirements per guidelines provided to Customer by Secureworks	R, A	I	
	Configure implementation rules on Customer side based on guidelines provided by Secureworks, Partner, or both, as applicable	R, A	I	
	Configure implementation rules in the Secureworks environment	I	R, A	
	Configure Endpoints (e.g., hosts, laptops) for Security Event logging	R, A	I	
	Test Agents before deployment	R, A	I	
	Install Agents	R, A	I	
	Configure connectivity to Secureworks-designated IP ranges and ports	R, A	I	
	Configure Secureworks Client Portal (and Red Cloak Portal, if applicable) access for Customer's authorized users	C, I	R, A	
	Configure CrowdStrike Falcon access for Customer's authorized users (initial configuration and creating initial administrator account); provide training for CrowdStrike Falcon if applicable	I	I	R, A
	Manage user accounts within CrowdStrike Falcon (e.g., create new accounts, apply appropriate permissions)	R, A		C
	Provide training (remotely) to Customer for Secureworks Client Portal and Red Cloak Portal	I	R, A	
	Provide Customer with access to CrowdStrike Falcon	I		R, A
	Provide Customer-side post-install validation steps to Customer (if applicable)	I	R, A	
	Complete Customer-side post-install	R, A	C, I	

AETD with CrowdStrike or AETD Elite with CrowdStrike				
Activity	**Task**	**Customer**	**Secureworks**	**Partner**
	validation steps (if applicable)			
	Complete Secureworks-side post-install validation steps	I	R, A	
Security Monitoring	Apply Secureworks analytics / Red Cloak watchlists to telemetry	I	R, A	
	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	
	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	R, A	C, I	

AETD with CrowdStrike or AETD Elite with CrowdStrike				
Activity	**Task**	**Customer**	**Secureworks**	**Partner**
	lists and alerting procedures through Secureworks Client Portal as needed)			
	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) for process disruption, hash banning, or host isolation prior to submitting a change request to Secureworks	R, A	I	
	Submit through Secureworks Client Portal (or otherwise contact SOC to submit) all change requests for in-scope changes; ensure requests are internally vetted and approved within Customer's organization, and include all information necessary to implement each request	R, A	I	
	Perform validation on completed changes	R, A	C	
	Notify Customer (through Secureworks Client Portal or email) that requested change was completed	I	R, A	
	Provide explicit pre-approval for Secureworks to implement emergency IP blocks without first obtaining Customer approval (optional)	R, A	C	
	Implement emergency blocking-rule changes as necessary (e.g., to address real-time malicious traffic on Customer's behalf)	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	R, A	I	

AETD with CrowdStrike or AETD Elite with CrowdStrike				
Activity	**Task**	**Customer**	**Secureworks**	**Partner**
	been implemented			
	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		
Support	Conduct troubleshooting related to the Service to determine root cause of an event flow disruption	C, I	R, A	
	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	R, A
	Provide support to Customer for issues relating to the Secureworks Client Portal (including mobile access) and Red Cloak Portal	I	R, A	
	Ensure Secureworks has current contact information for authorized contacts regarding Customer's account	R, A	I	
	Contact Partner for assistance with CrowdStrike troubleshooting	R, A		C, 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	R, A	C	

AETD with CrowdStrike or AETD Elite with CrowdStrike				
Activity	**Task**	**Customer**	**Secureworks**	**Partner**
	application store			
	Maintain network ranges (e.g., public, DMZ, and private) and network translation devices (e.g., NAT pools, proxies, and load balancers)	R, A	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	I	
	Maintain valid support contracts with Partner	R, A	I	

2.3.5.1 Partner Obligations

Secureworks' provision of this Service is dependent on specified Partner obligations identified herein; therefore, Secureworks shall not be liable for either Service delays such as latency in telemetry forwarding or Partner's failure to perform its obligations.

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:

- Secureworks Client Portal Training
- Secureworks Client Portal User Roles and Audit
- Escalation Procedures
- MPLE Rules Review
- Ticket Review and Baseline Secureworks Client Portal Reports
- Managed Device Alignment (e.g., ensuring understanding of expectations between Customer and Secureworks for 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 Secureworks Service-related documentation to Customer. Documentation is generally provided through the Secureworks Client Portal. Customer is responsible for obtaining CrowdStrike documentation and training from CrowdStrike.

2.4.1 Overview Training

If Customer purchases AETD Elite, then in addition to the previously described training, Customer will also be provided with overview training, which is a high-level overview of the Secureworks Client Portal, the Red Cloak Portal, and the CrowdStrike Falcon Portal as related to the Service. Secureworks will facilitate this webinar-based training that consists of the following topics:

- Event data flow
- Red Cloak Analytics
- Secureworks Client Portal with ticket review

Overview training focuses primarily on event data flow and Red Cloak Analytics.

2.5 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 described in the subsection(s) 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 SOW.

- Custom reports and customizing AETD-generated reports
- Custom watchlists or alerts
- Dedicated incident response services
- Installation and provisioning of CrowdStrike Agents and Red Cloak Inspector Modules
- Analysis of minor events
- Integration of complementary products that are not managed by Secureworks (e.g., anti-virus software, web reporting software)
- Vendor/Partner API Integration
- Remediation of malware and threat actor activity
- Alert suppression through vendor/Partner platform

3 Service Fees and Related Information

Service Fees are based on the number of Endpoints for which CrowdStrike Agents are purchased. 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 delivers 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.
  - **Threat Hunting:** See the Appendix for information about threat hunting.
    Note: If Customer purchases AETD with CrowdStrike, then Active Threat Hunting is an ***add-on*** service (threat hunting is included when Customer purchases AETD Elite with CrowdStrike).

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. Security Incidents generated from long-term correlation logic and retroactive analyses based on newly identified threat indicators are not subject to this SLA. Event(s) deemed low severity may be sent to Customer for review, and will be available through the Secureworks Client Portal for reporting.	1/30th of monthly fee for Service for the affected Device
Incident Investigations *(with Red Cloak)*	Upon generation of an AETD Red Cloak-based Security Incident designated by Secureworks as significant, Secureworks will provide an Incident Investigation within twenty-four (24) hours from the timestamp of creation of the Security Incident. 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	1/30th of monthly fee for Service for the affected Device

SLA	Description	Credit
	services through a separately signed Statement of Work.	
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., Secureworks Client Portal, mobile app) within one (1) hour from the creation time stamp on the ticket. 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 Secureworks Client Portal and the Red Cloak Portal shall equal no less than 99.9% of the time during any calendar month. "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. "Customer access to the Secureworks Client Portal and Red Cloak Portal" is defined as the ability of the Secureworks monitoring service to successfully log in to these portals. 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 Lifecycle Policy and Related Information

Secureworks provides its Lifecycle Policy online 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.

6.2 Secureworks-Provided Licenses for CrowdStrike Agents

If Secureworks provides the AETD licenses for CrowdStrike Agents, then Secureworks will:

- Invoice Customer in advance and procure the licenses per Customer request
- Receive and configure the licenses
- Facilitate renewal of the licenses (for an additional charge)

After Secureworks receives payment for the licenses from Customer, Partner will provide the licenses to Secureworks. Partner will provide support as related to the licenses.

6.3 Additional Service Features and Limitations

Feature/Limitation	Description
Data Retention	Secureworks will provide up to thirty (30) days of data retention in the Red Cloak Portal.
Non-standard Configurations	Secureworks will not support any non-standard configurations. Customers must ensure all connectivity requirement are met, including all web proxies and outbound controls, which includes allowing connectivity to required IP ranges and ports (Secureworks will provide to Customer).
Service Commencement	Service commencement will begin once telemetry is being received through Red Cloak Analytics.

Abnormal High Event Volume: If an abnormal amount of events are generated across the Endpoints being monitored, then Secureworks retains the right, in its sole and reasonable discretion, to conduct a purge that will remove all unnecessary event data that is beyond the thirty (30) day retention period as defined above, after the event data is analyzed and any threats are identified. If Secureworks determines that such a purge is required, then Secureworks will provide Customer with written notification after the purge has been successfully completed.

6.4 Red Cloak Inspector Module Installation, Management, Maintenance and Limitation of Liability

If Customer purchases AETD Elite with CrowdStrike, then the following applies to the Service:

1) The installation, ongoing management, and maintenance of the Red Cloak Inspector Module are the sole responsibility of Customer.
2) Customer can install and perform ongoing management of the Red Cloak Inspector Module by utilizing both the Red Cloak Portal and the Red Cloak Portal guide in combination with Customer's software distribution process.
3) The Customer is responsible for ensuring all Endpoints report into the Red Cloak Portal at least once every thirty (30) days. Any Endpoint that has not communicated properly in the last thirty (30) days will no longer be monitored, will not be included in other analytics, and will not be included in the total Endpoint count displayed in the Red Cloak Portal.
4) Secureworks will make available a list of supported Red Cloak Inspector Module versions. Secureworks will provide 60 days' notice of upcoming end-of-support for a given version. Any Endpoint that is past the end-of-support date will not be supported or allowed to be connected to the Red Cloak Portal.
5) SECUREWORKS WILL NOT BE RESPONSIBLE FOR ANY LOSSES, COSTS, OR DAMAGES RELATING TO THE INSTALLATION OF THE END POINT USER SOFTWARE. SECUREWORKS STRONGLY RECOMMENDS THAT CUSTOMER INSTALL AND EVALUATE THE RED CLOAK INSPECTOR MODULE 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.
6) SECUREWORKS WILL NOT BE RESPONSIBLE FOR ANY IMPACT THAT MAY BE INCURRED FROM INSTALLING RED CLOAK INSPECTOR MODULE ON AN UNSUPPORTED OPERATING SYSTEM OR CUSTOM BUILT IMAGE.
7) SECUREWORKS WILL NOT BE RESPONSIBLE FOR ANY IMPACT FROM CUSTOMER'S FAILURE TO COMPLY WITH THE RED CLOAK INSPECTOR MODULE UPDATING PROCESS.
8) 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 THE CUSTOMER.
9) 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 RED CLOAK PORTAL.

6.4.1 Endpoints and Contract Alignment

It is Customer's responsibility to ensure the contracted number of Endpoints on which Red Cloak Inspector Modules are installed is not exceeded. If at any time throughout the course of the agreement, Secureworks determines that Customer's total number of Endpoints exceeds the number of Endpoints contracted for, a change order will be required. The change order will reflect both the change in the number of Endpoints, and the corresponding increase in charges. Customer herby agrees to execute any such change order and to pay for any corresponding increase in charges.

6.4.2 Contract Termination and Red Cloak Inspector Module 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 Red Cloak Inspector Module 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 RED CLOAK INSPECTOR MODULES FROM ITS ENVIRONMENT AS OF THE TERMINATION DATE.

7 Appendix

7.1 Add-on Service Component: Active Threat Hunting ("ATH")

ATH is an add-on to the Service, and is for customers that need to understand their exposure to targeted threats. **If Customer purchases AETD Elite with CrowdStrike**, then Secureworks will conduct the ATH activities described herein. Secureworks-proprietary methodology, expertise, and intelligence will be used to identify advanced threat actors and their tactics, techniques, and procedures ("**TTPs**"). The threat hunters will attempt to identify existing adversary presence or threat actor TTP (or tradecraft) in Customer's environment. They will also review evidence that may persist in Endpoint systems and other relevant Customer Data, to identify indicators of compromise. ATH includes the following:

- Threat hunters will work closely with Customer to gain a thorough understanding of Customer's environment
- Review and escalate to Customer (using agreed-upon process) any critical activity that could represent a targeted compromise
- ***Weekly Hunting Report:*** Customer will receive a weekly summary report of the hunting activities and any notable findings that require further investigation
- ***Weekly Touchpoint Meetings:*** Secureworks will facilitate a weekly teleconference to discuss any findings or answer any questions that may arise (per Customer request, a different meeting cadence can be discussed)
- ATH information provided to Customer within the Red Cloak Portal (e.g., links to activity, investigations, and related ATH information will take Customer to the Red Cloak Portal)

Support for threat hunting is generally available Monday – Friday, 8 a.m. – 5 p.m. US Eastern Time, excluding US holidays.

Active Threat Hunting is not a replacement for Incident Response or a point-in-time Targeted Threat Hunt ("**TTH**"), which may involve deeper forensic analysis and eviction guidance. Customer can purchase advanced support through a separate, signed SO or Statement of Work.

Note: Currently, the Red Cloak Inspector Module for this Service can be installed on Windows and Linux Endpoints. Linux Endpoints are supported for AETD Elite, but the depth of active threat hunting available for these Endpoints is affected. See the Red Cloak Endpoint Agent Supported OS Versions information on the Secureworks website (https://www.secureworks.com/client-support/lifecycle-policy) for supported operating system versions.

Active Threat Hunting Priorities

While hunting, the threat hunters may also identify commodity malware, unauthorized software, and other Acceptable Use Policy ("**AUP**") violations; however, this type of activity is not part of threat hunting and Customer will receive notification through standard monitoring as described in section 2.2.1, Security Event Monitoring and Alerting. Weekly report content will vary based upon the findings with a focus on documenting and reporting on the most severe items first. The table below describes how threats are categorized.

Priority	Threat Type	Description
1	Targeted	Events or artifacts that may indicate the presence of an adversary within Customer's environment and requires immediate investigation.
2	Commodity	Events or artifacts associated with widely available malware or tools. This activity could pose a significant risk to Customer if not remediated. The threat hunters will assess the existence and use of such malware or tools based on evidence available to decide whether an additional escalation outside the standard monitoring services (described in Section 2.2.1) is needed.
3	AUP/Potentially Unwanted Program ("**PUP**")	Events or artifacts related to unwanted programs or activity that is generally prohibited in acceptable use policies (e.g., adware, remote access tools, and third-party chat clients).

The responsibility assignment matrix below describes the participation required by both Customer and Secureworks in completing tasks for ATH.

AETD Elite / ATH			
Activity	**Task**	**Customer**	**Secureworks**
Active Threat Hunting	Complete the pre-hunt questionnaire (Secureworks uses responses as part of executing hunting activities)	R, A	I
	Perform periodic review of Customer's Endpoints and related Customer Data to identify intrusion indicators	I	R, A
	Escalate intrusion indicators to Customer using agreed-upon escalation procedures	I	R, A
	Deliver threat hunting report to Customer (indicates notable activity observed)	I	R, A
	Schedule and conduct periodic meetings with Customer at agreed-upon interval to discuss findings and answer	C, I	R, A

AETD Elite / ATH			
Activity	**Task**	**Customer**	**Secureworks**
	questions		
	Investigate and remediate threats that Secureworks communicates to Customer; provide feedback to Secureworks about results from investigation and remediation	R, A	C, I

8 Glossary

Term	Description
Counter Threat Platform ("**CTP**")	A Secureworks proprietary MSS Services platform that ingests log data to produce events within the CTP system, 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.
Device(s)	Equipment that is in scope for the Service.
Due Diligence	Validating the accuracy of information used to create Customer's original Transaction Document against the actual environment in which Services will be performed.
End of Life ("**EOL**")	The date on which all support for a product ends, which includes any software upgrades, hardware upgrades, maintenance, warranties, or technical support.
End of Sale ("**EOS**")	The date on which a product is no longer available for purchase.
Endpoint	An Internet-capable computing machine or end unit such as a desktop computer, laptop, smart phone, tablet, thin client, or another similar device.
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.
Hosted Counter Threat Appliance ("**HCTA**")	Equipment that specifically allows Secureworks to collect data while performing a Secureworks-defined service for Customer, such as monitoring Customer's network and environment for security threats.

Term	Description
Identified Changes	Differences (e.g., Device quantity, make, model, software package, or software version) that are discovered while conducting due diligence for the Service.
Incident Investigation	The process and output of Secureworks examining a specific, in-scope security issue that arises and is escalated to Customer.
Multi-Purpose Logic Engine ("**MPLE**")	Secureworks proprietary tool that uses specific rules to identify, in real time, patterns that may indicate malicious activity.
Partner	The vendor that will be providing the CrowdStrike Agent and related support for this Service.
Red Cloak Inspector Module	Forensic scanner and investigation tool that provides CTU with a flexible environment to apply intelligence toward the detection of malware and threat actor activity.
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**")	A legally-binding arrangement to meet defined standards for the Service.