Secureworks®

SERVICE DESCRIPTION

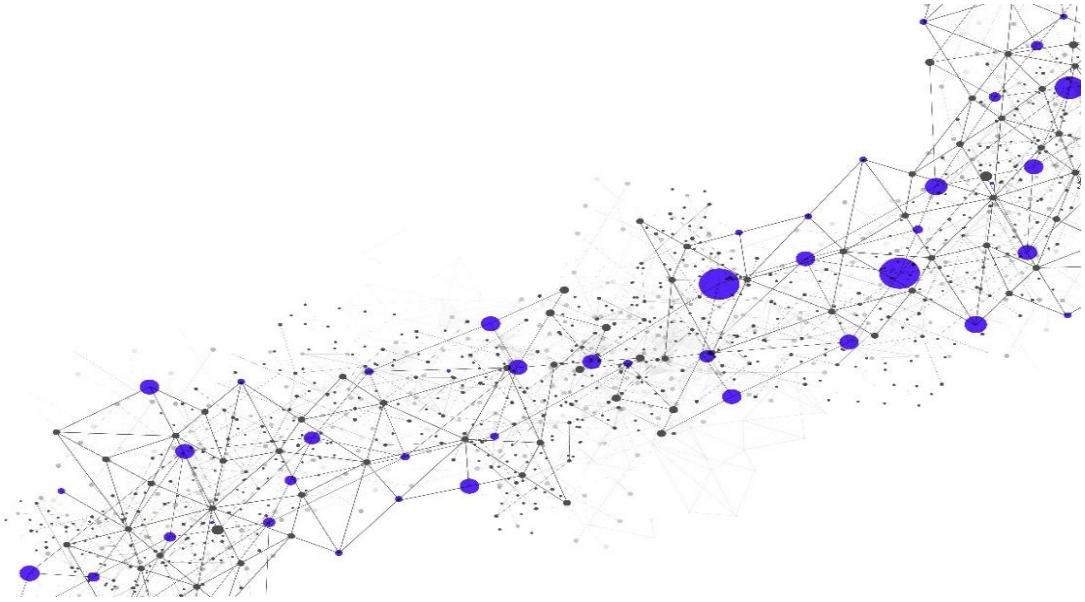
AETD with Microsoft Defender ATP*

Release Date

June 11, 2021

Version

2.1



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

*** Limited availability; please contact your Secureworks Sales Engineer for more details**

Table of Contents

1 Service Introduction

This Service Description ("**SD**") describes the Advanced Endpoint Threat Detection with Microsoft Defender Advanced Threat Protection 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 management functions, which can include changes (e.g., Multi-Purpose Logic Engine tuning, watchlist and suppression rule modifications), rule/policy modifications, upgrades (excluding Microsoft Defender Advanced Threat Protection; also referred to as "**Defender ATP**"), troubleshooting for Red Cloak™, and similar functions, upon Customer request. Secureworks will also monitor Security Events and Azure Event Forwarding to Secureworks, and alert Customer as applicable.

1.1 Overview

Secureworks will monitor one or more Microsoft Defender ATP Agents (referred to as "**Agents**" or "**Devices**" in this SD) that are licensed to Customer. Customer is responsible for procuring the appropriate number of software licenses for the Agents, including the required Azure Event Hubs and Azure Application, from Microsoft or an approved Microsoft third-party vendor ("**Partner**") for installing the Agents on Endpoints, and perform activities necessary to ensure log data (events) is sent to Secureworks systems for processing.

The Agents will send endpoint telemetry to Customer's tenant in the Microsoft Defender Security Center. Secureworks will obtain that endpoint telemetry, and it will be processed through the Secureworks Red Cloak Analytics System—which contains Secureworks Threat Intelligence ("**TI**"). In addition, native Microsoft events will be sent to the Secureworks Counter Threat Platform™ ("**CTP**") for Multi-Purpose Logic Engine ("**MPLE**") rule processing. The processing allows Secureworks 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. This Service 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
- Event Flow Monitoring and Alerting
- Integration with Customer's Tenant

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: Responsibilities for Devices (Customer and Secureworks), Maintenance Program, and Subscription Program.

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 Microsoft Defender ATP Agent(s) and Endpoints

Customer will do the following:

- Ensure the Endpoint entitlement licensed by Customer from Microsoft is not exceeded
- Manage configuration for Microsoft Defender Security Center
- Enable event forwarding to Secureworks from within Microsoft Defender Security Center
- Remediate all malware and threat actor activity (unless otherwise contracted with Secureworks through a separate Service Order)
- 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)
- Contact SOC to request assistance with host isolation or process disruption; Customer will manage prevention hashes and Endpoint threat prevention policies
- Provide written requests for isolating hosts as security response action
- Ensure all operating systems ("**OSs**") for the Agents that are in scope for the Service are supported by both Microsoft and Secureworks; ensure that only compatible OSs are used, and that the OSs meet the minimum software requirements of both Microsoft and Secureworks
- Ensure Endpoints have sufficient available resources for installation and operation of the Agent as defined by Microsoft's operating environment requirements
- Install the Agent on Endpoints, ensuring that the contracted number of Endpoints is not exceeded
- Upgrade or update Agent as needed; use a process to deploy upgrades/updates first in a test environment, and assess any impact before deploying software upgrades/updates to production Endpoints and environments
- Ensure that all Agents to be monitored are connected to the Microsoft Defender Security Center
- Manage and troubleshoot the Agent, which includes the following:
    - Conduct all required ongoing maintenance of Agent
    - Ensure availability of Agent
    - Monitor performance of Agent
    - Respond to and remediate issues with availability and performance of Agent
    - Reinstall Agent as needed
    - Conduct all troubleshooting of Agent
    - Remove all Endpoint Sensor Software from all Endpoints and Customer's environment by contract end or termination date
    - Ensure all Endpoints report into the Microsoft Defender Security Center 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 Connectivity

Customer will provide and maintain remote network connectivity to Customer's environment, including ensuring sufficient network bandwidth, and the in-scope Sensors that are necessary for Secureworks to perform the Service. SLAs will not apply to the Sensor(s) that are experiencing connectivity issues that are beyond the control of Secureworks.

1.2.3 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.

1.2.4 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 users is up to date with the Secureworks SOC. Customer is responsible for timely responses to tickets that Secureworks escalates to Customer through the Portal.

1.2.5 Maintenance

Customer will notify the Secureworks 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.

1.2.6 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.

1.2.7 Software Procurement

Customer will license the software necessary for Secureworks to deliver the Service. Customer will ensure that its software is at a version that is supported by Secureworks prior to provisioning of the Service and remains at versions that are Secureworks supported during the Subscription 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.

1.2.8 General

- Customer will ensure that Customer personnel are scheduled and available to assist as required for the Service.
- 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, and related information) 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(s).
- 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).

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 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). 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.

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
- **Prepare:** Baseline the project schedule, and identify required training; Customer provides information necessary to execute implementation for MSS Services
- **Execute:** Complete configuration of HCTA(s) and related service-enabling technology, validate ingestion of identified log source(s) if applicable, schedule and deliver foundational training, and activate services
- **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 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 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 Portal
- Collect Customer information that is necessary for implementation
- Complete provisioning and installation activities (e.g., sending Devices to Customer, configuring Devices within the Secureworks Counter Threat Platform ("**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

2.2 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 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 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. Customer-created custom alerts can be configured for monitoring and alerting. Customer can submit a Service Request to Secureworks, and Secureworks will work with Customer to evaluate the request and determine how to proceed. 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	Upon receiving alerts that are triggered by Devices, Secureworks will process all Security Events 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 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 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 require immediate attention and/or represent potential business impact to Customer environment (e.g., targeted

Ticket Severity	Description
	threats, opportunistic malware infection)
Medium	Security Events that do not require immediate attention and typically represent pre-compromise, compliance, audit, reconnaissance, or other types of activity that is unlikely to indicate a significant threat to Customer environment
Low	Security Events that may represent a misconfigured security control, false positive-prone countermeasures, and other activity that has little to no impact to Customer environment

* ***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 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 Statement of Work ("**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 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.

2.2.1.5 Security Event Reporting

Customer can use the 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 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 Portal.

- Secureworks will attempt to identify the cause of the event flow disruption. If the issue is related to Microsoft, the customer will be responsible for contacting Microsoft support.
- If the root cause of the EFD is not related to the Service (e.g., a Customer-side network change or Agent misconfiguration), then Secureworks will advise Customer to troubleshoot issues directly with the vendor, 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 Integration with Customer's Tenant

Customer will receive a welcome kit that contains instructions for the integration between CTP and Microsoft Defender Security Center. The integration enables secure transmission of Endpoint

telemetry and events from Microsoft Defender Security Center. Customer must configure Azure Event Hubs, Azure Application, and Microsoft Defender Security Center as part of the integration.

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 Hosted Counter Threat Appliances ("**HCTAs**") 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 Hosted Counter Threat Appliance ("**HCTA**")

The Service requires an HCTA for data collection and monitoring.

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.
- 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 with Microsoft Defender ATP				
Activity	**Task**	**Customer**	**Secureworks**	**Partner**
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	
	Create and provide to Secureworks the escalation procedures to follow for tickets (Customer will modify as needed at any time through the Portal)	R, A	I	
	Enter Customer's initial escalation procedures into Portal	A, C, I	R	

AETD with Microsoft Defender ATP				
Activity	**Task**	**Customer**	**Secureworks**	**Partner**
	Provide to Customer the implementation guidelines for service implementation	I	R, A	
	Ensure managed Device(s) meets Secureworks-provided hardware and software specifications prior to the start of implementation	R, A	C, I	
	Prepare the environment as required to implement the Service	R, A	I	
Service Implementation	Provide Secureworks with access to Customer's Defender ATP tenant	R, A	C, I	
	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	
	Work with partner to resolve installation issues for Agents (if applicable)	R, A		C, I
	Provide Portal training	I	R, A	
	Complete post-install quality check	R, A	I	
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	C, I	R, A	

AETD with Microsoft Defender ATP				
Activity	**Task**	**Customer**	**Secureworks**	**Partner**
	escalation procedures			
	Conduct log correlation to identify internal sources/destinations of traffic related to escalated Security Incidents (if applicable)	I	R, A	
	Submit ticket through 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 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	Submit through Portal (or otherwise contact SOC to submit) all change requests for managed Devices; ensure requests are internally vetted and approved within Customer's organization, and include all information necessary to implement each request	R, A	I	
	Perform maintenance that is specific to Customer's environment and implement Customer-submitted change requests during Customer-designated maintenance window	C, I	R, A	
	Notify Customer (through Portal or email) that requested change was	I	R, A	

AETD with Microsoft Defender ATP				
Activity	**Task**	**Customer**	**Secureworks**	**Partner**
	completed			
Support	Conduct troubleshooting related to the Service to determine root cause of an event flow disruption	C, I	R, A	
	Notification of an event flow incident through the Portal ticket with optional auto-E-mail or auto-SMS text notification ***Note:*** Auto-SMS is out of scope in Japan.	I	R, A	
	Provide support to Customer for issues relating to the Secureworks Client Portal (including mobile access) and Red Cloak Portal	I	R, A	
	Work with Partner to troubleshoot and resolve issues with Agents	R, A		C, I
	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	
	Download and register mobile application (named "Secureworks Mobile") to mobile device from an application store	R, A	C	
	Maintain valid vendor support contracts for Defender ATP service	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 Service delays or failures arising out of 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:

- Portal Training
- Portal User Roles and Audit
- Escalation Procedures
- MPLE Rules Review
- Ticket Review and Baseline Portal Reports

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 Portal.

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. Upon request, Secureworks can provide out-of-scope technical support on a time and materials basis pursuant to a separate SO or SOW.

3 Service Fees and Related Information

Service Fees are based on Customer's total number of Endpoints. 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 targeted threat hunting.

5 Service Level Agreements ("SLAs")

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

SLA	Definition	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 Portal for reporting.	1/30th of monthly fee for Service for the affected Device
Incident Investigations *(with Red Cloak)*	Upon generation of a Security Incident from AETD Defender ATP that is 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 defines as non-critical are performed at the discretion of Secureworks and with no associated SLAs. Some requests may be referred to professional services under a separately signed Statement of Work.	1/30th of monthly fee for Service for the affected Device
Availability	Communications availability to the Internet and Customer access to the 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 Portal and Red Cloak Portal" is defined as the ability of the Secureworks monitoring service to successfully log in to these portals.	1/30th of monthly fee for Service each day in which the Service fails to meet this SLA

SLA	Definition	Credit
	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.	
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. 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

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 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.

7 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 Service Order 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.
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.
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.
Identified Changes	Differences (e.g., Device quantity, make, model, software package, or software version) that are discovered while conducting due diligence for the Service.
Multi-Purpose Logic Engine	Secureworks proprietary tool that uses specific rules to identify, in real time,

Term	Description
("**MPLE**")	patterns that may indicate malicious 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.