Secureworks®

SERVICE DESCRIPTION

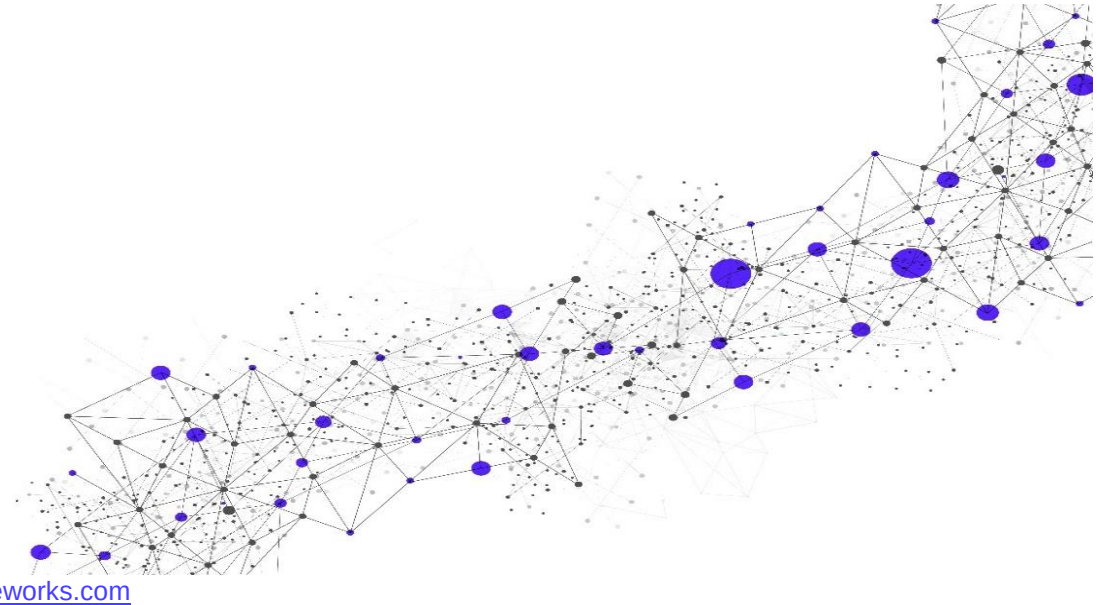
Advanced Remediation Management (ARM)

Release Date

August 13, 2021

Version

11.1



www.secureworks.com
A Dell Technologies Company

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

Table of Contents

Copyright

1 Service Introduction

This Service Description ("**SD**") describes the Advanced Remediation Management ("**ARM**") 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.

1.1 Overview

Secureworks will provide Customer with Ticket-based Level 2 ("**L2**") support for managing and investigating security-related Tickets. A concurrent subscription to at least one Managed Security Service that is based on the Secureworks Counter Threat Platform™ ("**CTP**") is a prerequisite for this Service.

Secureworks L2 security analysts will review and manage an agreed-upon monthly count of Tickets ("**Baseline Monthly Ticket Volume**") as specified in Customer's Transaction Document. If the agreed-upon monthly count is not consumed in a given month, then the remaining ticket count for that month is forfeited and cannot be consumed in any subsequent month. During the Customer-selected Service Delivery Hours (12x5 or 24x7) specified in the Transaction Document, Secureworks will conduct activities for the Baseline Monthly Ticket Volume as specified in an agreed-upon Operations Guide. See Section 2.2, Service Implementation, for information about the Operations Guide.

Customer's processes, procedures, and security Platforms within Customer's information technology ("**IT**") environment will be used in conjunction with Secureworks proprietary security tools, processes, and procedures to perform the Service. Secureworks will provide integrated service implementation, Security Incident investigation and analysis, and remediation management as described herein. Secureworks will provide the Service for one Environment. An Environment is defined as:

- A maximum of three of the following ticket sources:
  - CTP through the Secureworks Client Portal
  - Customer's internal Ticketing System (e.g., maximum of one system such as ServiceNow, Remedy, or Resilient)
  - Maximum of one designated shared email inbox within Customer's internal email system or one Email security system – for "Phishing Tickets"
- One group of Customer's Platforms that are deployed within Customer's Environment for L2 security analysts to access as part of conducting the Service

  Important Note: The total number of Platforms in this group cannot exceed 18, ***including*** Customer's internal Ticketing System and one designated shared email inbox. For example, if Customer's internal Ticketing System will be in the group, then this counts as one of the 18 Platforms, and Customer can have 17 additional Platforms; however, if both Customer's internal Ticketing System and one designated shared email inbox will be in the group, then Customer can have 16 additional Platforms. Also, only one Security Information and Event Management ("**SIEM**") system can be included in the maximum of 18 Platforms (i.e., multiple SIEMs cannot be included in one Environment).

- One CTP instance (queue)
- Up to **12** use case Workflows (e.g., for malware or phishing), depending on Customer's capabilities, that will be documented in the Operations Guide
- One set of Customer Processes (the agreed-upon Operations Guide)
- One Customer point of contact ("**POC**") for operational governance when managing and investigating security-related Tickets
- One network that is accessible through a single virtual private network ("**VPN**") or single point of remote entry

The Service includes the following primary components:

- **Security Incident investigation and analysis:** Investigate and analyze Tickets through use of Customer's Platforms and Secureworks tools, including applying threat intelligence ("**TI**") from the Secureworks Counter Threat Unit™ ("**CTU™**")
- **Remediation management:** Provide prescriptive guidance and recommendations to Customer for modifying security controls and identifying Incidents requiring Level 3 ("**L3**") actions
- **Program governance:** Provide monthly reports and updates to Customer about L2 security operations capabilities and processes, help ensure achievement of Customer's Service objectives, and work with Customer to conduct activities and meetings as applicable to the Service

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

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 Objectives ("**SLOs**") 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 Services and/or SLOs, or a transition to monitor-only Services.

1.2.1 Connectivity

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

1.2.2 Access

- Customer will leverage the connectivity solution proposed by Secureworks. Customer will provide and maintain remote network connectivity to the device(s) necessary for Secureworks to perform the Service. Customer will communicate any network or system changes that could impact service delivery by submitting a ticket in the Secureworks Client Portal ("**Portal**").
- Customer will provision a reasonable number of requested user accounts for Secureworks in a timely manner, for all in-scope security Platforms used by Secureworks employees.
- Customer will provide appropriate access to Customer's service/help desk, as required by Secureworks to perform the responsibilities defined herein.
- Customer will provide appropriate access privileges to Customer's internal Ticketing System to extract raw data used for service performance measurements.
- Customer will provide raw data to Secureworks based on a format acceptable to Secureworks or as otherwise agreed, in scenarios where access cannot be provided.

1.2.3 Customer Documentation and Process Walkthrough

- Customer will have Platforms and security controls in place to monitor, detect, report, and respond to security events. Secureworks will not deploy security controls as part of the Service.
- Customer will provide access to existing data sources and Platforms to support incident investigation for analysis and remediation management.

1.2.4 Customer Platforms Documentation and Training

- Customer will validate the security Platform list with Secureworks on a periodic basis
- Customer will facilitate and sponsor training sessions for any new Platforms or technologies, if/when existing Platforms and technologies are replaced, or scope is expanded.
- Customer will identify a single POC for each Platform and ensure the POC's availability for required sessions during Service Implementation.

1.2.5 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 interval 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 Points of Contact and Initial Implementation Scheduling

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

2 Service Details

The subsections below contain details about the Service, including service delivery hours, implementation, and steady state (the "**Ongoing Operations**").

2.1 Service Scheduling

To begin the Service, Secureworks will do the following:

- Contact Customer's POC within ten (10) Business Days after execution of Customer's Transaction Document to schedule the initial meeting; initial meeting must occur within 60 calendar days after execution of Customer's Transaction Document (see Section 4.1 for details)
- Schedule Service Implementation to begin with a minimum of four (4) weeks after the initial meeting
- Use commercially reasonable efforts for completing delivery of Service according to Customer's need
- Send an email confirmation of an agreed-upon schedule (Customer replies to email with confirmation, and this constitutes formal acceptance of such schedule)

Secureworks requires that once scheduling of any on-site work at Customer's facility has been mutually agreed to, any changes Customer makes to the schedule or on-site work within two (2) weeks of the on-site work to be performed will incur a $2,000 re-scheduling fee. This re-scheduling fee does not apply to work that does not require travel by Secureworks.

2.2 Service Implementation

Secureworks will guide Customer through a series of steps to set up the processes, procedures, and related work instructions that will be used to deliver the Service. Secureworks contextualizes and customizes the Service to Customer's processes, procedures, and Environment. Secureworks will work with Customer to set up, initialize, and enable the service delivery team to leverage the existing in-scope Platforms within Customer's Environment, including testing the processes, procedures, and related work instructions. Below are key activities required for completion of Service Implementation.

- Discuss and agree on Service Implementation timeline(s) and schedule(s)
- Establish the required connectivity and access to Customer's network and in-scope Platforms for service delivery
- Document access requirements
- Introduce Customer to the ARM Program Governance function
- Obtain and/or document Customer's current operational processes
- Align with Customer's security operations processes and overall security strategy
- Clarify roles and responsibilities
- Review deliverables that Secureworks will provide to Customer (RACI and Workflows)
- Define an Operations Guide
- Define Service objectives for Ongoing Operations

The timeline for Service Implementation is approximately 12 to 16 weeks. Meeting this timeline depends on collaboration between Customer and Secureworks to ensure necessary Customer resources are available for all activities during Service Implementation. The process consists of three phases and corresponding activities:

- Discovery
- Integration
- Stabilization

Each phase and corresponding activities are explained in the subsections below.

2.2.1 Discovery

Secureworks will schedule the initial meeting with Customer (occurs through remote teleconference). During this meeting, date(s) and time(s) for the initial on-site workshop / discovery sessions will be scheduled, and Customer will identify the appropriate POCs within Customer's organization and ensure their availability is secured for the duration of implementation.

Secureworks will conduct the on-site workshop / discovery sessions at a Customer-designated location. Customer will provide Secureworks with names and contact information for individuals from whom Secureworks can obtain required information for the Service.

- **Environment Discovery:** Secureworks will work with Customer to obtain and document key Environment information such as network infrastructure diagrams, and Customer's current information security and Incident Response ("**IR**") processes, procedures, and Workflows

2.2.2 Integration

Customer and Secureworks will work together to establish remote connectivity between Customer's IT environment and Secureworks. Customer and Secureworks will also work together to complete operational integration activities (e.g., creating user accounts for Secureworks to access Customer's IT environment) and do the following:

Define Current State: Develop a description of Customer's current "AS IS" IT environment and related operations.

Define Future State: Develop a description of Customer's future "TO BE" IT environment and related operations to align with Customer's security operations processes and overall security strategy.

Develop Operations Guide: Create the Operations Guide as the basis for Ongoing Operations to achieve Customer's future state.

2.2.3 Stabilization

During this phase, Customer and Secureworks will test processes and team interactions that will be used during Ongoing Operations. Secureworks will work collaboratively with Customer to ensure any issues that may affect Ongoing Operations are identified.

2.3 Ongoing Operations

Upon completion of Service Implementation, Secureworks will perform the appropriate subset of activities listed in the subsections below for Ongoing Operations, based on Customer's needs.

2.3.1 Investigate, Analyze, Contain and Resolve

Secureworks will conduct the activities listed in the subsections below

2.3.1.1 Investigate

- Identify event correlation and validation from multiple sources (e.g., CTP + anti-virus, CTP + SIEM, CTP + firewall log)
- Triage security tickets to determine true positive ("**TP**") or false positive ("**FP**")
- Recommend fine tuning for non-actionable events from CTP
- Detonate suspicious samples in sandbox and extract Indicators of Compromise ("**IOCs**") and Indicators of Attack ("**IOAs**") relevant for the event
- Provide Security Incident escalation, determining incident impact from a technical perspective (not reputational or financial impact, for example)
- Provide Security Incident analysis and Customer-specific context (e.g., individual host versus VP laptop versus critical production server / investigating host name, user account activity, and operating system)

2.3.1.2 Analyze

- Manage the investigation and analysis of Security Incidents based on Tickets from Ticketing Sources
- Monitor ticket sources during Customer-selected Service Delivery Hours
- Perform incident prioritization, triage, and remediation management
- Discuss and clarify aspects of the Security Incident information with Secureworks Level 1 ("**L1**") Security Operations Center ("**SOC**") or Customer L1 SOC
- Perform unscripted analysis activities, with access to Secureworks tools and Customer's Platforms to provide valuable business context to alerts discovered
- Perform incident analysis by correlating data from various sources to determine if a critical system or data set has been impacted
- Incident follow-up through resolution with detailed triage notes

- Re-classify Security Incidents according to Customer-provided Security Incident severity ratings

2.3.1.3 Coordinate and Expedite

- Coordinate containment
- Expedite short-term containment recommendations or actions in accordance with agreed-upon policies and procedures to limit the damage of an ongoing Security Incident

2.3.1.4 Resolve

Tickets will be considered resolved and/or closed as explained below.

- **False Positive:** Tickets are closed as false positives if the incident or event is determined to be a false positive by the ARM team and no additional action is required
- **True Positive:** Tickets are closed as true positives if the Security Incident or event was verified as a True Positive by the ARM team.

2.3.2 Remediation Management

Secureworks will support Customer in remediating Security Incidents through performing the activities listed below.

- Escalate eradication and recovery to the relevant Customer groups
- Recommend Operations Guide updates to Customer, and improvements to Customer's processes
- Recommend new MPLE rules or tuning of Customer's specific rules
- Consult with Customer's IR team

2.3.3 Program Governance

The Secureworks Program Management Office ("**SPMO**") will provide Program Governance for the Service. At the start of the Stabilization phase during Service Implementation, a Secureworks Security Delivery Manager ("**SDM**") commences Program Governance activities

Customer will designate a POC that will work with the SDM for the duration of the Service. The POC will be responsible for enabling coordination across Customer's organization for resolving Security Incidents and other activities for ongoing operations. The POC will also provide information for secondary contacts in case the POC is unavailable.

Listed in the table below are tasks for which Customer is responsible.

Governance Area	Task
General Communication and Scheduling	• Coordinate scheduling of all personnel required for the Service
Escalations	• Manage escalation of issues between Customer and Secureworks with appropriate information provided by Secureworks to manage the escalation. • Work together in good faith with Secureworks to agree on resolution for any disagreements regarding whether specific tasks not listed are in scope
Change and Corrective Actions	• Mutually agree with Secureworks on Change Control procedure

Listed in the table below are tasks for which Secureworks is responsible.

Governance Area	Task
General Communication and Scheduling	• Provide communications to ensure stakeholders are involved, expectations are accurately set and managed, and key stakeholders are informed as necessary • Work with identified stakeholders to ensure Customer and Secureworks are progressing with mutually agreed upon responsibilities and action items • Conduct meetings to communicate roles and responsibilities, review assumptions, and schedule activities, which include organizing regular operational reviews of activity, performance metrics, and active issues • Maintain a log of active issues indicating responsibilities for Customer and Secureworks (by personnel) and share such log with Customer monthly
Escalations	• Manage escalation of issues between Customer and Secureworks for timely closure in accordance with a defined mutually agreed process • Work with Customer to agree on resolution for any disagreements regarding whether specific tasks are in-scope
Change and Corrective Actions	• Implement changes in compliance with mutually agreed upon Change Control procedure • Initiate corrective action, when required, to manage risks and issues with proposed mitigation plans

2.3.3.1 Program Governance Methodology

The Secureworks Program Governance Methodology is a phased approach for continual improvement of the Service. The table below contains the phases and general tasks.

Program Governance Phases	
Initiate	• Initiate program-based approach • Define organizational structure and key stakeholders • Define governance framework based on people, process, and technology
Stabilize	• Reach a stabilized operational stage based on people, process, and technology • Implement governance frame addressing the current state of services • Develop baseline metrics and processes
Continuous Improvement	• Support Customer in defining roadmaps and creating business cases for enhancing the security services • Identify and recommend service improvement initiatives

2.3.3.2 Governance Framework

The Secureworks Program Governance approach stabilizes the in-scope services, maximizes the effectiveness of these services, and delivers continuous improvement of the services by using a mutually agreed-upon Governance Framework.

2.3.3.3 Governance Meetings and Reviews

The review meetings in the table below define the framework of the participants and the responsibilities and agenda of those roles that are responsible for the administration of the governance processes. Both parties should mutually agree upon, in writing, the following draft recommendation.

Governance Meeting		Details
Weekly Operations Review	**Chaired by**	Customer
	General Topics	Operational activities completed in the prior week
		Planned operational activities for next week
		Reporting: Ticket count and high-level analysis; lessons learned; statistics for High, Medium, and Low tickets (per SLOs)
		Issues and risks
Monthly Service Review	**Chaired by**	Secureworks Program Manager
	General Topic	Ticket Reporting: • Ticket quota against subscription • Service Level Objective ("**SLO**") adherence for Managed Security Service-specific tickets (only applicable to 24x7 Service Delivery Hours) Overall services status • Performance and stability Continuous improvement and growth • Threat landscape addressing SLOs (from ARM / L2 in context of Service)
		Issues/Risks – Service perspective
		Scope Review: • Scope change • Review if any tools and / or technologies have changed If Yes, Secureworks Program Manager and Customer shall determine best course of action
		Service improvement tracker and plan - focus areas addressing action items and escalations

2.3.4 Customer and Secureworks Responsibilities

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

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

ARM Service			
Activity	**Task**	**Customer**	**Secureworks**
Ongoing Operations	Recommend industry best practice security monitoring and event management service policies	I	R, A, C
	Provide L2 security event management services in accordance with established policies on basis of coverage documented in Transaction Document	C, I	R, A
	Notify Customer of Security Incidents and escalate to Customer's security function	C, I	R, A
	Perform functional escalation to any relevant group (e.g., IT, Incident Response team, Customer's SOC) per the agreed runbooks	C, I	R, A
	Recommend countermeasures for Security Incidents	A, I	R, C
	Provide reporting on Security Incidents with mutual agreement	C, I	R, A
	Resolve security violations internal to Customer	R, A	C, I
	Resolve and notify security violations internal to Secureworks	I	R, A, C
	Configure and manage security Platforms	R, A, C	I
	Coordinate and interact with business users and third parties	R, A, C	I
	Implement and configure network connectivity and access related credentials for providing Information Security Analysis Services.	R, A	C, I
	Test and confirm network connectivity and access related credentials	C, I	R, A
	Provide access to non-Secureworks Platforms for security analysis and reporting	R, A	C, I

ARM Service			
Activity	**Task**	**Customer**	**Secureworks**
	Develop and maintain Operations Guide	C, I	R, A
	Provide information for development of Operations Guide	R, A	C, I
	Coordinate Security Incident response (e.g., teleconferences, communication within Customer's organization regarding the Security Incident)	R, A	C, I

2.4 Business Days and Related Information

Business Days for Secureworks global headquarters are Monday – Friday and Business Hours are 8 a.m. – 5 p.m. US Eastern Time, excluding United States holidays. These hours are applicable to Service Scheduling (see Section 2.1).

Listed in the table below are the hours for the Stabilization phase, and the hours for Ongoing Operations for both Service Delivery Hour options (12x5 and 24x7).

Note: During the Stabilization phase, SLOs do not apply.

Model	Hours
12x5	Monday – Friday, 12 hours per day (10 a.m.to 10 p.m. Eastern European Time - *UTC +2 Hours During Standard Time, +3 Hours During Daylight Savings Time)
24x7	24 hours a day, 7 days a week
Stabilization Phase	Monday – Friday, 8 hours per day (10 a.m. to 6 p.m. Eastern European Time - *UTC +2 Hours During Standard Time, +3 Hours During Daylight Savings Time)

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 may provide out-of-scope technical support on a time and materials basis pursuant to a separate Transaction Document.

2.5.1 Out-of-Scope Workflows

- Perform Industrial Control System ("**ICS**") / Supervisory control and data acquisition ("**SCADA**") workflows
- Provide audit and compliance workflows
- Monitor for wire fraud

2.5.2 Out-of-Scope Investigation

- Reverse malware engineering (static malware analysis, decompiling and extracting signatures based off the sample collected)
- Monitor or investigate any tickets not generated from the three agreed-upon ticket sources
- Create, test, or deploy Intrusion Detection System ("**IDS**") / Intrusion Prevention System ("**IPS**") signatures
- Install IDS, IPS, and firewall inline
- Provide/perform firewall or IT network configuration changes
- Conduct user account removal
- Alter trust relationships (revoke trusted certificates, two-factor authentication / "**2FA**")
- Implement NULL routing

2.5.3 Out-of-Scope Remediation

- Restore from backups
- Validate host compliance and/or declare incidents complete
- Remove any mitigating controls set in the containment phase
- Install new security software or equipment
- Perform root cause analyses

2.5.4 General Out-of-Scope Activities

- Deliver security awareness training
- Provide user account provisioning
- Platform management activities: Installing, configuring (Examples: developing SIEM correlation rules, tuning SIEMs, adding SIEM sources), updating, assuring uptime, backup, and availability of Customer's security Platforms
- Create or implement IT security policies or procedures
- Segment IT networks
- Create or update asset inventory
- Provide Level 1 MSS or TI services; ARM analysts will not work events or notable events directly from a third-party SIEM – Ticketing System integration is required
- Provide L3 and/or Level 4 ("**L4**") support services
- Provide "on-call" analysts outside of normal Service Delivery Hours
- Perform "Eyes-On-Glass" monitoring of alerts or events activity
- Manage Customer-owned platforms (deployment, configuration, ruleset management, software license management)
- Maintain Customer devices or applications, including servers, network devices, application IDs, management consoles, server patches, endpoint, and anti-virus updates
- Execute recommended remediation
- Eradicate identified security breaches
- Create custom correlation rules in Customer's SIEM

- Install third-party software on any appliance or system, unless explicitly indicated in Section 2 as being part of the Service.

3 Service Level Objectives

The SLOs listed in the table below are only applicable to Tickets from CTP, the 24x7 option for Service Delivery Hours, and Tickets within the Baseline Monthly Ticket Volume.

Ticket Priority	High	Medium	Low
Response Time	2 Hours	8 Hours	24 Hours
Target Threshold	95%	90%	85%
Measurement	Time between CTP ticket assignment to ARM team and start of investigation, as measured by Secureworks systems	Time between CTP ticket assignment to ARM team and start of investigation, as measured by Secureworks systems	Time between CTP ticket assignment to ARM team and start of investigation, as measured by Secureworks systems
Frequency	Monthly	Monthly	Monthly

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 SLOs set forth above are subject to the following limitations:

- Ongoing Operations has commenced; SLOs **do not** apply during Service Implementation (which includes the Stabilization phase).
- 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 SLOs shall not apply during scheduled maintenance outages.
- 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 SLOs shall not apply if any act or omission by Customer prohibits or otherwise limits Secureworks from providing the Service or meeting the SLOs, 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 SLOs 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 SLOs with respect to any Incident response or help desk ticket request are also dependent on Secureworks' ability to connect directly to Customer-Side Technology on Customer's network.
- The SLOs 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.

4 Service Fees and Related Information

Service Fees are based on Customer-selected Service Delivery Hours (12x5 or 24x7) and the Baseline Monthly Ticket Volume. See Customer's MSA or CRA (as applicable), and Transaction Document for details, including the following:

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

4.1 Related Information

- The term of the Service shall commence on the Start of Service date. The initial meeting (through remote teleconference) will occur within 60 days after executed Transaction Document. If the initial meeting does not occur within 60 days despite repeated attempts from Secureworks to meet with Customer, then the 60th calendar day after executed Transaction Document will be deemed the official "Start of Service" date.
- Customer will be invoiced the first of each month that the Service is being provided. The first month of Service will be pro-rated based on the Start of Service date. The period from the Start of Service to the end of the calendar month will be added to and invoiced along with the second month's (which is the first full-service month) invoice.
- During Ongoing Operations, if Customer exceeds the Baseline Monthly Ticket Volume, a charge defined in the Transaction Document is assessed. No charges will apply if Customer exceeds the Baseline Monthly Ticket Volume before commencement of Ongoing Operations.
- The Service shall terminate after the period specified in the Transaction Document.

4.2 Adjustments to Baseline Monthly Ticket Volume

After reaching Ongoing Operations, Customer and Secureworks can review the Baseline Monthly Ticket Volume once every three months. Baseline Monthly Ticket Volume can be re-established per Customer request through following the Change Order Process. The Baseline Monthly Ticket Volume cannot be reduced in the first year of the contract. Baseline Monthly Ticket Volume is limited to standard volumes as defined by Secureworks.

5 Glossary

Term	Definition
Authorized Security Contacts	List of Customer's authorized contacts with whom Secureworks will engage.
Baseline Monthly Ticket Volume	An agreed-upon count of monthly tickets that Secureworks L2 security analysts review and manage. This is established with the Transaction Document, and can be re-established through following the Change Order Process and submitting a change order.
Change Order Process	Secureworks sales operations process for changing an original Transaction Document, which requires a request from Customer to Secureworks through email, and Secureworks creates an addendum for an existing Transaction Document.
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	Internal team of security experts that research and analyze threat data across

Term	Definition
("**CTU**")	Secureworks global Customer base and actively monitors the threat landscape. Provides TI that extends visibility into cyber threats beyond the edges of the networks of Secureworks Customers. The TI, applied to technology and the Secureworks suite of services, enables Customers to expand visibility and reduce the time it takes to see and respond to them, thereby resisting and avoiding cyberattacks.
Customer Processes	A collection of related, structured activities or tasks that in a specific sequence produces an output/serves a defined purpose for Customer. A process may often be visualized (modeled) as a flowchart (Workflow) of a sequence of activities with interleaving contact, escalation, and decision points.
Designated Services Contacts	Customer list of appointed points of contact for each department containing Authorized Security Contacts.
Environment	A technical security ecosystem defined by a common set of characteristics.
Indicators of Compromise ("**IOCs**") and Indicators of Attack ("**IOAs**")	Artifacts observed on a network or in an operating system that with high confidence indicate an attempted or confirmed computer intrusion.
Incident	An information security matter needing intervention of human intelligence to determine the next course of action.
Level 1 Support ("**L1**")	Alert monitoring, detection, and ticket creation service (not part of the Service).
Level 2 Support ("**L2**")	Investigative service for ticketed alerts and the coordination of activities in response to validated threats. Level 2 examines security tickets and event information and manually correlates or researches them using various security Platforms deployed within Customer's IT environment.
Level 3 Support ("**L3**")	Remediation activities based on enriched tickets escalated by L2.
Level 4 Support ("**L4**")	IR, forensics, containment, and eradication activities.
Operations Guide	Collection of Workflows specific to Customer (also referred to as a runbook). Contains additional information such as the following: • Customer contact information • RACI matrix • Customer Platforms
Phishing Tickets	Tickets created based on a user-reported email that leads to an investigation. Multiple instances of phishing or spam campaigns, or other suspicious email, that causes a potential threat to Customer, may be recorded as multiple tickets. Secureworks can decide to track these types of emails as a single ticket should they occur within the span of eight (8) hours and one of the following conditions apply: • Emails are part of the same campaign, having the same sender or subject or content; or

Term	Definition
	• Emails are part of a pre-planned test or security awareness training exercise related to phishing emails.
Platform	One software application in Customer's Environment that Secureworks may interact with as part of delivering the Service: • Security investigation tool • Monitoring of one or multiple devices, by collecting events, performance data, logs, tickets, etc. • Communication between Service delivery teams (both Customer and Secureworks) • Security control Specific examples of Platforms are as follows: • IDS/IPS • Security Information and Event Management • Anti-virus • Advanced Endpoint Protection / Endpoint Detection and Response ("**EDR**") • Vulnerability scanner • Network Packet Capture ("**PCAP**") / network analysis • Threat intelligence platform • Ticketing • Proxy • Phishing or Email security system • Collaboration Tools Multiple versions of a software tool will be counted as multiple Platforms (e.g., three versions of one software tool will be counted as three Platforms).
Secureworks Center of Excellence ("**SCoE**")	Location of L2 support for the Service.
Secureworks Client Portal ("**Portal**")	The Portal is the online site for all Managed Security Services Customers. It is where Customer and ARM team will conduct some activities (e.g., case management and metrics for Security Incidents) for the Service. 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.
Security Information and Event Management ("**SIEM**")	Process of identifying, monitoring, recording, and analyzing security events or incidents within a real-time IT environment.
Security Operations Center ("**SOC**")	Secureworks maintains a SOC with locations in the United States and internationally. Secureworks administers security services and support from this SOC, such as monitoring Security Events, aggregating and correlating data, conducting analysis, escalating Security Events, and performing other security-related activities. The SOC provides L1 support and works with the ARM team.
Service Level	A specific measurable characteristic to meet defined service delivery standards.

Term	Definition
Objective ("**SLO**")	
Start of Service	The date of the initial meeting (occurs through remote teleconference) between Customer and Secureworks, and is the date on which Secureworks begins implementing the Service as described in this SD.
Ticket(s)	A request for action to be taken to respond to an information security event or alert related to an event. For ARM, a ticket is any request for a single L2 security investigation.
Ticketing System	Software that collects all Customer support requests from different sources for management in one location.
VDI	Virtual Desktop Infrastructure, or VDI, refers to the platform needed for operating a user desktop inside a virtual machine located on a server in the data center.
Workflow	The sequence of steps that an L2 analyst conducts as part of L2 Security Event Management Services for events generated by one of the agreed-upon three ticket sources.