Secureworks

SERVICE DESCRIPTION

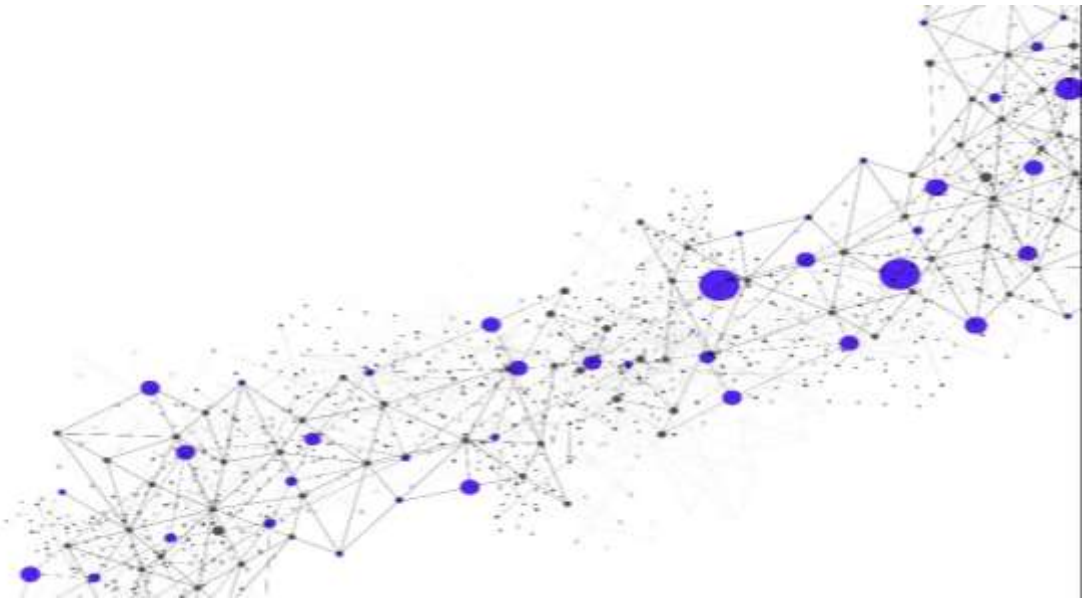
Vulnerability Program Management – VMS Platinum

Release Date

November 26, 2024

Version

17.2



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 the Vulnerability Program Management – Vulnerability Management Scanning Platinum 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.

1.1 Overview

Secureworks will provide Customer with professional services to design and build Customer's vulnerability management ("**VM**") program. If Customer has an existing VM program, then Secureworks will help Customer improve its program. See Section 2.1.4, VM Program Development, for details about developing a program and improving an existing program.

In addition, on an ongoing basis, Secureworks will provide the following:

- Vulnerability program management
- Recurring (scheduled) and on-demand vulnerability scanning and reporting
- Remediation guidance

Vulnerability scans can be conducted for Hosts/infrastructure (including virtual machines), policy compliance (e.g., Security Configuration Assessment), and/or websites. Host/infrastructure scans and policy compliance scans use IP addresses, and website scans use universal resource locators ("**URLs**"). Secureworks will use modules within the vulnerability scanning tool (also referred to as the "**scanning tool**") to conduct scans, as applicable. See 2.2.3, Configuration and Scanning Management, for more information about scanning.

A Customer-provided vulnerability scanning subscription and/or license from Taegis VDR Qualys, Tenable, or Rapid 7 is required for vulnerability scanning and reporting. A ***license*** is the software that is deployed in order to use a tool – e.g., the Business Intelligence ("**BI**") Reporting Tool requires a license to be installed on a virtual machine, and a vulnerability scanning subscription requires a license. A ***subscription*** is software as a service for an online vulnerability management tool, such as Qualys.

If Customer does not have an existing vulnerability scanning subscription and/or license through Taegis VDR, Qualys, Tenable, or Rapid 7, then Customer can purchase vulnerability scanning licenses (for Qualys or Taegis VDR only) through Secureworks. See the Appendix in this SD for Service details that are specific to Qualys. Customer acknowledges and agrees that if Customer purchases the Qualys license through Secureworks, such license shall be provided under Qualys' standard terms that accompany the license; see the details in the Appendix. Customer owns the Qualys subscription and can independently use the subscription without interacting with Secureworks. Customer can complete tasks such as conducting on-demand scans and managing exclusions at Customer's risk – e.g., Customer would need to determine the best time to conduct an on-demand scan, the scope of the scan, and whether the scan needs to be conducted during a scheduled change window. Customer acknowledges and agrees that if Customer purchases the Taegis VDR license through Secureworks, such license shall be provided under Secureworks' standard terms that accompany the license.

For remediation guidance, Secureworks will prioritize vulnerabilities and provide suggested remediation actions according to Customer's business and vulnerability management requirements. Secureworks will also work with Customer's internal and/or third-party IT operations teams to track progress against remediation actions.

Listed below are required items for the Service, and the quantity for each item will be defined in Customer's Transaction Document.

- Number of Customer representatives (technical owners)
- Number of IP addresses to be managed
- Number of vulnerability scanners
- Host infrastructure scanning/reporting cycle (monthly, every two months, or quarterly)
- Policy compliance and/or Security Configuration Assessment ("**SCA**") scanning and reporting (number of IPs)
- Policy compliance and/or SCA reporting cycle
- Number of websites/web applications
- Website scanning/reporting cycle (monthly, every two months, or quarterly)
- Number of On-Demand Scans for vulnerabilities or websites per scan cycle*****
- Number of meetings per month (each meeting of up to one hour timeframe, e.g., meetings with technical owners to report on remediation actions)*****
- Number of Host/infrastructure scanning changes per scan cycle*****
- Number of policy compliance changes per scan cycle*****

***** ***Note:*** *The last four items in the above list are outputs/required items that are determined based on the aforementioned items in the list.*

The Service includes the following components:

- Vulnerability Program Management (during ongoing operations)
- Maintenance of Customer's Technical Environment for VM
- Configuration and Scanning Management
- Remediation Guidance Activities
- Reporting

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

Vulnerability Scanning Acknowledgement: Customer acknowledges that Secureworks services cannot identify weaknesses in network architecture (other than any identified during Service activation based on the documentation made available by Customer) or weaknesses in general application architecture. Secureworks does not guarantee that all vulnerabilities on every tested system or application will be discovered. Secureworks does not guarantee that there will be no false positives. The nature of vulnerability scanning is such that some vulnerabilities and misconfigurations of Customer devices (e.g., un-patched Hosts or the use of older, unsupported versions of software) can pose risks when scanned. Secureworks cannot guarantee that Host/infrastructure vulnerability assessments will not adversely affect the performance or availability of the target systems. Service level objectives ("**SLOs**") are defined below.

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 the obligations listed below. Noncompliance with Customer obligations relative to this Service may result in suspension of managed components of the Service and/or SLOs, or a transition to monitor-only components of the Service.

1.2.1 Assets in Scope

Customer will provide and maintain the accuracy of the list of Assets required to execute scanning activities described in Section 2.2 of this SD. This includes providing the minimum information required by the vulnerability scanning tool.

1.2.2 Data Backups

Customer acknowledges and agrees that the scanning of IP addresses and/or domain names may expose vulnerabilities and, in some circumstances, could result in the disruption of Service or corruption or loss of Customer Data. Therefore, Customer will perform regular backups of all Customer Data contained in or available through the devices connected to Customer's IP address(es) and/or domain names should backups need to be used to restore data.

1.2.3 Cloud-Based IP Address Acknowledgement

Customer acknowledges that the IP address of any cloud-based asset is subject to change. Customer will identify the specific IP addresses of cloud-based Assets that are to be scanned and will update this information for the vulnerability scanning tool or notify Secureworks through submitting a Service Request when any IP address for a cloud-based Asset changes, and Secureworks will update the information for the vulnerability scanning tool.

1.2.4 Ownership and Authority for IP Addresses

Customer will use the Service to only scan the IP addresses owned by and registered to Customer, or for which Customer has the full right, power, and authority to consent to have the Services scan and/or map. Customer may not rent, lease, or loan the Service, or any part thereof, or permit third parties to benefit from the use or functionality of the Service through timesharing, service bureau arrangements, or otherwise. If one or more of the IP addresses identified by Customer are associated with computer systems that are owned, managed, and/or hosted by one or more third-party service providers, then Customer represents that it has the consent and authorization from each service provider as necessary for Secureworks to perform the Service. Customer agrees to facilitate any necessary communications and exchanges of information between Secureworks and each service provider.

1.2.5 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 the Secureworks IP range to Customer location(s) and online platforms (such as cloud-based tools to be used for service delivery – e.g., the scanning tool) as applicable to the Service. Service Level Objectives ("**SLOs**") will not apply to the Device(s) that is experiencing connectivity issues that are beyond the control of Secureworks.

1.2.6 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.

1.2.7 Communications

Customer will communicate with Secureworks through email or an agreed-upon ticketing system. Customer should submit all Service-related issues or requests using the agreed communication method. Customer will also submit timely responses to communications escalated by Secureworks to Customer through the agreed communications method.

1.2.8 Maintenance

Customer will notify Secureworks through the agreed communications method at least two (2) Business Days in advance of any Customer-side network maintenance or system changes that could affect service delivery to enable Secureworks to avoid unnecessary issue escalations to Customer.

1.2.9 Usage Overage

Quantities/deliverables are fixed according to Customer's Transaction Document; however, if Customer needs additional quantities/deliverables ("**Overage**"), then Customer can purchase them in groups of 10, and Customer will pay for the Overage as applicable (see Transaction Document for charge).

1.2.10 Provisioning in a Public Cloud or Private Virtual Environment

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

1.2.11 Hardware and Software Procurement

Customer will purchase or lease the hardware and license the software necessary for Secureworks to deliver the Service. Customer will ensure that its hardware and software are updated to the latest versions prior to provisioning the Service and remains at versions that are supported during the Services Term. Secureworks SLOs 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.

1.2.12 Customer Representatives or Technical Owners

Customer will provide Secureworks during the first month of the engagement with contact information for the defined total number (as indicated in the Customer's Transaction Document) of customer representatives and/or technical owners that will be engaged for the Service. Customer will update the contact information with Secureworks as needed to maintain Service delivery. If the ***total number*** of Customer representatives or Technical Owners change, then Customer will need to work with Secureworks to submit a Change Order.

1.2.13 General

- Customer will ensure that Customer personnel are scheduled and available to assist as required for the Service(s).
- Customer will have obtained consent and authorization from the applicable third party, in form and substance satisfactory to Secureworks, to permit Secureworks to provide the Service if Customer does not own network resources such as IP addresses, Hosts, facilities or web applications.

- Customer will provide to Secureworks all required information (key personnel contact information, credentials, and related information) prior to work being started.
- Customer will promptly reply to all requests from Secureworks.
- Customer-scheduled downtime and maintenance windows will be communicated to allow adequate time for Secureworks to perform the Service and adjust deliverables.
- 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 deny list).
- Customer will uninstall all licensed tools, return all leased hardware, and disable any accounts provided for Secureworks to perform the Service upon termination of the Service. This includes the installed BI Reporting Tool, associated licenses, and software provided within the contract.
- Customer will do the following:
    - Implement all security patches (Customer personnel will need to implement these patches as applicable)
    - Provide a list of contacts for the locations where the in-scope vulnerability scanner appliances are installed
    - Identify the in-scope IPs and excluded IPs for scanning
    - Identify sensitive areas (e.g., manufacturing domains and compliance-specific domains such as for PCI) and work with Secureworks to establish the limitations (e.g., rules for scanning sensitive areas) for both scanning and remediation
    - Provide Secureworks with credentials for authenticated scanning and website scanning
        - If credentialed scans are used, then Customer must ensure that provided credentials are accurate and correct for each of the systems that must be scanned, and address any issues associated with scan credentials.
    - Enable Secureworks to access Customer's asset database and/or similar organization tool (required for appropriate tracking of remediation)
    - Provide the vulnerability scanners and valid subscription(s) or license key(s); Taegis VDR, Qualys, Tenable, and Rapid 7 are the scanners that can be used for this Service
    - Ensure proper installation and configuration of the scanners, and connectivity to the scanner vendor's platform

  Delays or absence of customer participation and adherence to the above will directly impact Secureworks' ability to adhere to the Project Plan, target delivery date, maturity of the VM Program, quality of service, and overall service delivery. Secureworks reserves the right to revisit the initial scoping and update costs if needed.

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

Customer will provide licenses (for vulnerability scanning) for this Service, or purchase licenses from Secureworks. The subsections below contain details about the Service and how it will be implemented.

2.1 Service Implementation

The service implementation period begins with the initial meeting and ends when the Service and devices supporting the Service are transferred to the Secureworks Steady State team.

The subsections below describe Transition Management (a Transition Manager will be assigned to Customer for end-to-end management of Customer's implementation), and the Secureworks implementation methodology for this Service (VM Program Management), which can be reasonably adjusted to meet Customer needs at the sole discretion of Secureworks. If Customer purchases Qualys licenses from Secureworks, then see Qualys Scanning Subscription Implementation in the Appendix for information about additional Service Implementation steps. As part of implementation, Secureworks will help ensure Customer understands how to use the Service through collaborative meetings and training.

Note: *Secureworks does not provide SLAs or SLOs for completing implementation within a specified period of time; the duration of the implementation is dependent on several factors, such as the maturity of Customer's current governance and operational processes, complexity of Customer's environment, clarity of Customer's requirements, and the ability of Customer to provide Secureworks with requested information within a mutually agreed-upon time period.*

2.1.1 Transition Management

Transition Management is provided to achieve Customer's business objectives within the agreed-upon constraints specified in this SD. A Transition Manager will be assigned to Customer and this manager will leverage standard, industry-recognized project management tools and methodologies (e.g., PMI PMBOK, ITIL Framework) to manage implementation and help transition Customer to ongoing operations. The Transition Manager will contact Customer to schedule the initial meeting.

The Transition Manager will be responsible for the following:

- Serve as Customer's primary point of contact at Secureworks for the duration of the implementation period
- Oversee all aspects of the VM Program Development process, including outcomes, action items, roles, and responsibilities
- Create governance and related documentation including the Project Plan for monitoring/managing delivery against scheduled tasks
- Organize and conduct key meetings including initial meeting, discovery, design, acceptance, and ongoing reviews to provide status of scheduled tasks, issues, and risks
- Establish accountability across program resources, manage issues and risks through project RAID, and ensure expectations are accurately set and managed as necessary
- Manage implementation exceptions within known tolerances of time, cost, risk, scope, and resources
- Establish communication and foster decisions across stakeholder groups keeping everyone informed, involved, and aligned
- Work with Customer to resolve any disagreements on in-scope services and tasks
- Ensure build and integration of the service solution for acceptance and transition to Customer and/or Secureworks steady state team
- Manage changes associated with this agreement in compliance with mutually agreed-upon Change Control procedures
- Manage escalation of issues between Customer and Secureworks to a timely closure in accordance with a defined mutually agreed-upon process

- Ensure outcomes of all phases of VM Program Development are achieved – e.g., creation of clear requirements
- Ensure Customer provides Secureworks with appropriate access and connectivity to all Customer tools and systems that are necessary to deliver the Service

2.1.2 Implementation Governance

Customer will assign a project manager (or lead point of contact), and they will work with the Transition Manager to provide project management oversight and ensure performance of the responsibilities and obligations during implementation.

The key components of implementation governance include the following:

- Executive Sponsorship
- Stakeholder Participation
- Defined Roles and Responsibilities
- Standard Project Management Framework
- Established Communication Plan
- Weekly Progress Reviews and Reporting
- Monthly Project Steering
- Risk, Issue, and Escalation management
- Invoice management
- Contract management

2.1.2.1 Customer Responsibilities and Expectations

For the implementation, Customer agrees to do the following:

- Assign a technical POC for the duration of the Engagement to support activities (***Note:*** *Customer can assign a single person to be both, a project manager and a technical POC if desired; however, the assigned person must have technical knowledge to support activities*.)
- Assign and provide a list of key contacts from identified functional areas, as required
- Collaborate with Secureworks to create and approve Service Implementation deliverables in scope
- Partner with Secureworks to jointly govern the overall project and participate in technical work sessions as needed
- Partner with Secureworks to track and manage the escalation of issues between Customer and Secureworks with appropriate information provided by Secureworks
- Work with Secureworks in good faith to resolve any disagreements on in-scope services and tasks
- Provide reasonable assistance, cooperation, timely decisions, and support in connection with provisioning the Services being provided by Secureworks
- Coordinate the scheduling of required Customer stakeholders and ensure their participation in workshops and other core meetings
- Obtain any necessary internal or external permissions (including Customer's third-party providers) to share documentation with Secureworks
- Provide existing VM Governance documentation such as corporate policies, standards, organizational charts, and criticality matrix for Customer's current operating model upon request
- Provide existing VM Operational documentation such as workflows, playbooks, and RACI matrix for Customer's current operating model upon request
- Provide existing VM Toolset design and configuration documentation such as scanner placement design, Scan Configuration, Agent collection, Authentication Scanning, Reporting and System Integration for Customer's current operating model upon request

- Provide existing Infrastructure documentation such as Network diagrams, Asset and Application Inventory for Customer's current operating model upon request
- Provide existing supporting IT Management process documentation such as Patch Management, Incident Management, Change Management and Knowledge Management for Customer's current operating model upon request
- Provide permission and timeframes (vulnerability scanning windows) for Secureworks to perform initial scanning and discovery activities
- Obtain all consents, approvals, and licenses required by Secureworks, and/or Customer suppliers, licensors, and lessors that are necessary to support Service Implementation
- Prepare the target facility including rack, power, network any related infrastructure for all devices that are in scope for the Secureworks services
- Install devices, including connectivity, power sources, configuration validation and testing
- Review deliverables thoroughly and notify Secureworks of any required changes or additions
- Provide written acceptance of deliverables and signoff for successful completion of each phase
- Obtain executive acceptance of all organizational policies and procedures defined in the structure of the VM program
- Be accountable for Customer-internal adherence to organizational policies and procedures defined in the structure of the VM program

Customer shall have two weeks from the request date to provide any documentation or approval required by Secureworks related to the Service.

Delays or absence of customer participation and adherence to the above will directly impact Secureworks' ability to adhere to the Project Plan, target delivery date, maturity of the VM Program, quality of service, and overall service delivery. Secureworks reserves the right to revisit the initial scoping and update costs if needed.

2.1.2.2 Review and Acceptance of Implementation Deliverables

Within two (2) weeks of completing a deliverable within this project, Secureworks will issue draft deliverable documentation to Customer designated point of contact. Customer shall have two (2) weeks from delivery of such draft documents to provide comments (the "**Deliverable Review Period**"). If there are no comments received from Customer before the expiration of the Deliverable Review Period, the document shall be deemed final and Secureworks will finalize for distribution. For any deliverable, up to two (2) iterations are in scope.

2.1.3 Scope and Limitations for Implementation

Secureworks will provide professional services to support the development or improvement of Customer's VM Program to an initial state where it can be successfully operated and further evolved during ongoing operations.

References to initial configuration indicate where a subset of the future state scope will be built during Implementation.

The tables below show the options, parameters, and limits that will be specified within Customer's Transaction Document for the Service.

VM Technology Scope (D&B and Onboarding)	
Vulnerability Management Platform =	[Taegis VDR/Qualys/ Tenable/Rapid 7]
Vulnerability Mgmt. (Host/infrastructure scans) =	Yes or No
Policy Compliance (configuration scans) =	Yes or No

VM Technology Scope (D&B and Onboarding)	
Website Vulnerability Management =	Yes or No
Number of Scanning Appliances =	Up to X*
*** Volumes are defined in Customer's Transaction Document for this Service.**	

Definitions:

- **Vulnerability Management Platform** indicates the VM Toolset vendor among Taegis VDR, Qualys, Tenable, or Rapid 7 that Customer is using.
- **Vulnerability Mgmt. (Host/infrastructure scans)** indicates whether the Vulnerability Management module is in scope for Service Implementation.
- **Policy Compliance (configuration scans)** indicates whether the Configuration Compliance module is in scope for Service Implementation.
- **Website Vulnerability Management** indicates whether the Web App Scanning module is in scope for Service Implementation.
- **Number of Scanning Appliances** indicates the maximum number of scanning appliances that can be configured as part of initial configuration.

VM Development Scope for Processes (D&B and Onboarding)	
Number of Governance Processes =	Up to X* or Onboarding-only
Number of Operational Processes =	Up to X* or Onboarding-only
*** Volumes are defined in Customer's Transaction Document for this Service.**	

Definitions:

- **Number of Governance Processes** indicates the maximum number of Governance Processes to be developed or improved during Service Implementation, within the following VM Governance Processes areas:
  - Corporate Vulnerability Management Policy
  - Vulnerability Identification Standard
  - Vulnerability Assessment Standard
  - Vulnerability Remediation Standard
  - Exception Management Standard

  If it is determined that no development of Governance Processes is required due to Customer having a complete VM Program, then the Transaction Document will indicate "*Onboarding-only*."
- **Number of Operational Processes** indicates the maximum number of Operational Processes to be developed or improved during Service Implementation, within the following VM Operational Processes areas:
  - Asset Discovery and Categorization
  - Scan Configuration and Execution
  - Ad-Hoc Scanning

- Scan Impact
- Vulnerability Analysis and Prioritization
- Threat Intelligence Integration
- Vulnerability Remediation Orchestration
- Critical Vulnerability Handling
- Monitoring and Escalation
- Vulnerability Remediation Exception Management
- False / Positive Handling
- Risk Acceptance Handling
- Scan Exclusion Handling
- Vulnerability Findings Reporting
- Integrated Risk Posture Reporting

If it is determined that no development of Operational Processes is required due to Customer having a complete VM Program, then the Transaction Document will indicate "*Onboarding-only*."

VM Initial Configuration Scope (D&B and Onboarding)	
Number of IP Addresses (VM)	Up to X* or Onboarding-only
Number of Websites to Onboard (Web Application Scanning/WAS)	Up to X* or Onboarding-only
Number of Configuration Policies (PC)	Up to X* or Onboarding-only
Number of Asset Classes/Categories or VDR Tags	Up to X* or Onboarding-only
Number of Scan Profiles (VM)	Up to X* or Onboarding-only
Number of Scan Schedules	Up to X* or Onboarding-only
Number of Report Configurations	Up to X* or Onboarding-only
Number of VM System Integrations =	Up to X* or Onboarding-only
Number of VDR User teams =	Up to X* or Onboarding-only
*** Volumes are defined in Customer's Transaction Document for this Service.**	

Definitions:

- **Number of IP Addresses (VM)** indicates the maximum number of IP addresses that are in scope of the Service.
- **Number of Websites to Onboard (WAS)** indicates the maximum number of web applications to set up as part of initial configuration.
- **Number of Configuration Policies (CP)** indicates the maximum number of configuration policies to be built as part of initial configuration.

- **Number of Asset Classes/Categories** indicates the maximum number of asset categories to be built as part of initial configuration.
- **Number of Scan Profiles (VM)** indicates the maximum number of scan profiles to be built as part of initial configuration.
- **Number of Scan Schedules** indicates the maximum number of scan schedules to be built as part of initial configuration.
- **Number of Report Configurations** indicates the maximum number of report configurations to be built as part of initial configuration.
- **Number of VM System Integrations** indicates the maximum number of system integrations to be configured as part of initial configuration.
- **Number of VDR User teams** indicates the maximum number of VDR teams (user groups) to be configured as part of initial configuration

If it is determined that no Initial Configuration is required due to Customer having a complete VM Program, then the Transaction Document will indicate "*Onboarding-only*."

Note: When "*Onboarding-only*" is used in the Transaction Document, Customer is acknowledging that its current VM Program is 100% complete. All Governance and Operational Processes are assumed to be complete. The Onboarding process will be limited to facilitating transition of Customer's existing VM Operations to Secureworks (i.e., Vulnerability Program Management / VMSP). Secureworks will not perform any initial Toolset configuration.

2.1.4 VM Program Development

As part of implementation, Secureworks will use its expertise in developing Threat and Vulnerability Management ("**TVM**") programs for global organizations to help Customer design and build a VM Program, or help Customer improve an existing program, as explained below. See Section 2.1.1, Transition Management, for information about management oversight that Secureworks provides for designing and building a VM program, or helping Customer improve an existing program.

Note: If "*Onboarding-only*" is used in the Transaction Document, then Customer acknowledges that they have an existing and complete VM program and Secureworks will help onboard Customer to VMSP services only. Secureworks will not help Customer design, build, or improve its existing VM Program. See the note in the previous section for more information.

Designing and Building a VM Program: Secureworks will design and define a vulnerability management program. Secureworks will work with Customer to understand its infrastructure, security goals, and vulnerability posture, then provide vulnerability management processes and protocols for Customer and/or Secureworks to implement. This will enable more efficient implementation of the Service to achieve Customer's vulnerability management goals. Customer and Secureworks will do the following:

- Plan and support installation of new or additional vulnerability scanners (physical rack and stack is Customer's responsibility)
- Define and document VM processes and methodologies for Customer (including process for on-demand scans and reports)
- Develop Initial Configuration of VM technology toolset based on customer scale and needs
- Design VM tool for Integration with Customer's third-party tools (e.g., configuring Customer's VM scanners to work with ServiceNow; however, configuring ServiceNow is out of scope)

- Identify gaps that can be used to develop a program roadmap of future improvements to Customer's VM program
- Ensure Customer's readiness for efficient implementation of remaining Service components (e.g., Vulnerability Management Scanning Platinum, or "**VMS Platinum**" or "**VMSP**")

Improving an Existing VM Program: If Customer has an existing but incomplete VM program, then Secureworks will help Customer improve the program. This will enable more efficient implementation of the Service to achieve Customer's vulnerability management goals. Customer and Secureworks will do the following:

- Review and optimize placement of current vulnerability scanners (physical rack and stack is Customer's responsibility)
- Review and optimize Customer's VM processes and methodologies (including process for on-demand scans and reports)
- Review and optimize configuration of VM technology toolset based on customer scale and needs
- Design VM tool for Integration with Customer's third-party tools (e.g., configuring Customer's VM scanners to work with ServiceNow; however, configuring ServiceNow is out of scope)
- Identify gaps that can be used to develop a program roadmap of future improvements to Customer's VM program
- Ensure Customer's readiness for efficient implementation of remaining Service components (e.g., VMSP)

The subsections below explain the phases of the VM Program Development implementation process that Secureworks will use to help Customer ***create a VM program***. Secureworks will use the same process – as applicable – to help Customer ***improve an existing VM program***.

2.1.4.1 Phase 1: Discovery

Secureworks will analyze the existing functions that comprise Customer's VM Program, including governance, technology, infrastructure management, and operations. Secureworks will conduct interviews, review existing tools, processes, and policies, and build a document that describes the ***current state*** of Customer's program. VM program discovery is broad-based and is aligned with, but not limited to, best practices for standard VM frameworks. Listed below are the key responsibilities of Secureworks during this phase.

- Conduct VM Program Discovery workshop
- Conduct a Toolset / Architecture Review and Analysis up to the quantities of platforms, modules, scanning appliances and system integrations defined in the Transaction Document
- Conduct Review and Analysis of Customer's Governance and Operational processes up to the quantities defined in the Transaction Document; VM process areas are defined in Section 2.1.3, Scope and Limitations for Implementation
- Conduct Scanner Placement Review and Analysis of Vulnerability Scanners
- Develop recommendations for solutions to close the gap for integration into the Secureworks VMS Platinum Service
- Develop a project plan to deliver solution based on agreed-upon recommendations

2.1.4.2 Phase 2: Design

Secureworks will document the future state of the Customer's Vulnerability Management Program. Based on the agreed-upon recommendations from Phase 1 as accepted by Customer, Secureworks consultants will develop the solution design to be used during Phase 3, Build. Listed below are the key responsibilities of Secureworks during this phase.

- Develop detailed requirements for Customer's Governance and Operational processes for up to the quantities defined in the Transaction Document; VM process areas are defined in 2.1.3, Scope and Limitations for Implementation
- Develop Scanner Placement Design documentation for Vulnerability Scanners up to the quantity defined in the Transaction Document, including:
  - Zone/Environment placement diagram
  - Target/Scope Information (IPs/Hosts/Networks)
  - Network access requirements (for traffic across FWs)
- Design Scan Schedule Configurations up to the quantity defined in the Transaction Document according to Customer-defined configuration parameters (option profile, frequency, scan duration window, authentication, and other parameters).
- Design Report Configurations up to the quantity defined in the Transaction Document and within the constraints of the Toolset reporting features.
- Design VM Tool for Integration with Customer's VM third-party tools as defined in the Transaction Document, such as:
  - Asset Management System / Configuration Management Database ("**CMDB**")
  - Ticketing System

Note: Secureworks will not design or configure third-party tools beyond the VM Toolset

- Identify gaps that can serve as input into a roadmap to evolve the Customer's VM program across the following VM functional areas:
  - Governance
  - Technology (VM Toolset)
  - Infrastructure Management
  - Operations

2.1.4.3 Phase 3: Build

Secureworks will coordinate VM technology deployment and build the processes, playbooks, policies and governance models defined in Phase 2 above. The documentation from this activity will be used by the Customer's steady state delivery team. Listed below are the key responsibilities of Secureworks during this phase.

- Document or Update Customer's Governance and/or operational processes and procedures up to the quantities defined in the Transaction Document; VM process areas are defined in Section 2.1.3, Scope and Limitations for Implementation
- Provide support and coordination for installation of scanners up to the quantity defined in the Transaction Document
  Note: Customer is responsible for installing scanning appliances (hardware, virtual appliances, agents). Secureworks will provide support and coordination through detailed instructions, remote configuration of the BI Reporting Tool, and teleconferences.
  - Rack and stack support/coordination with on-site resources
  - Troubleshooting

- Provide support and coordination for System Integrations between Customer's Vulnerability Management Toolset and external supporting systems as defined in the Transaction Document, such as:
  - Asset Management System / CMDB
  - Ticketing System
- Develop initial scan configuration (e.g., frequency, schedules, authentication) of Toolset up to the quantity defined in the Transaction Document for:
  - Scanners/ Edge servers
  - Scan Modules
  - Scan Profiles
  - Scan Schedules
  - Asset Classes/Categories/VDR Tags
- Provide Report Development up to the quantity defined in the Transaction Document within the constraints of the Toolset reporting features
- Confirm with Customer connectivity of the scanners, which consists of Customer and Secureworks validating all scanners and components of the Service are transmitting data as expected

2.1.4.4 Phase 4: Integrate

Secureworks will work with Customer to ensure that the transition to steady state (ongoing operations) is successful. Customer and Secureworks will review the work products developed in Phase 3 and validate that the developed processes and technology perform as expected and meet the requirements identified. Listed below are the key responsibilities of Secureworks during this phase.

- Review Design Documentation for completeness
- Review Governance and/or Operational Process Documentation for completeness
- Test Procedures for Readiness and address Issues
- Handover to steady state team and complete Readiness validation
- Monitor Enablement of VMSP services and support stabilization
- Obtain Final Solution Acceptance and initiate steady state Operations

2.2 Service Components

The subsections below contain information about the components of the Service. A list of component that are included in the service will be available in the Transaction Documents mentioning the components or parts of the components that are included in the Service and will supported as highlighted below:

2.2.1 Vulnerability Program Management (during ongoing operations)

After implementation is completed, Secureworks will provide program management for managing delivery of the Service to Customer to ensure appropriate technical delivery, communication, and updates between Customer and Secureworks. A Secureworks program manager will focus on planning, delegating, monitoring, and overall management of all aspects of the Service to achieve Customer's business objectives within the standard constraints of time, cost, and quality. The program manager will work with the delivery professionals tasked with completing Customer's project to ensure proper transition to ongoing operations.

The scope of program management includes the following:

- Develop and confirm with Customer and Secureworks personnel the timeline for deliverables during ongoing operations
- Act as Customer's primary point of contact during ongoing operations
- Align responsibilities with Customer during ongoing operations to ensure Secureworks will be able to successfully complete and deliver in-scope activities in a timely manner
- Monitor and manage ongoing service delivery against the defined scope, to include schedule (e.g., for scans, reports, meetings), budget, and quality requirements
- Obtain approval from Customer and Secureworks on scope definition and ensure acceptance from Customer for completed deliverables
- Facilitate communications to ensure stakeholders are involved, expectations are accurately set and managed, and key stakeholders are informed as necessary
- Work with Customer to identify and address issues or concerns that impact service delivery
- Provide Customer with periodic updates on progress
- Provide periodic governance for reviewing program quality and success

During ongoing operations, Secureworks will follow an ITIL Service Management approach to achieve the following objectives:

- Identify areas of improvement and opportunities relative to Customer's security operations
- Make recommendations that Secureworks believes will benefit Customer regarding technical advancements, process improvements, and the threat landscape
- Support and participate in a mutually agreed-upon Service improvement program for continuous improvement

2.2.1.1 Governance Model (Ongoing Operations)

The table below defines the standard governance framework that is used during Customer's ongoing (steady state) operations. Customer and Secureworks can work together to customize the framework, and both parties shall mutually agree upon, in writing, the finalized governance model that will be used.

Meeting	Details	
Monthly Service Review	**Chaired by**	Secureworks Account Management team
	Required Attendees	Secureworks: Account Management team, Delivery Manager, Service Team Lead
		Customer: Security Director, Infrastructure Operations Director, Service Manager(s) and Vendor Management Office
	Agenda	Overall Service status – Red, Green and Yellow
		Issues/Risks – Service perspective
		Customer infrastructure vulnerability trends
		Service improvement plan - Focus areas addressing action items/escalations
		Roundtable/Action Items

Quarterly Service Review	**Chaired by**	Customer CISO or equivalent
	Required Attendees	Secureworks: Account Management team, Delivery Manager, VMS Platinum team Lead
		Customer: Security Operations Director, Security Engineering Director, Service Manager(s) and Vendor Management Office
	Agenda	Strategic improvements
		Executive Summary
		Scope of Work Review • Scope Change • Determine whether any IPs/applications have changed; Customer and Secureworks Program Manager will determine course of action for changes
		Program Governance Issues
		Service Improvement Tracker
		Performance and Stability

2.2.2 Maintenance of Customer's Technical Environment for VM

Secureworks will provide Vulnerability Program Management of Customer's defined Technical Environment for VM. The table below indicates Customer's options that will comprise the Technical Environment. All volume, time, and inclusion parameters (items with "Yes/No") will be specified in Customer's Transaction Document for this Service.

Customer's Technical Environment (Steady State)	Volume/Timing/Yes or No
Number of Customer representatives (technical owners)	Up to X*
Number of IP addresses to be managed	Up to X*
Number of vulnerability scanners	Up to X*
VM Infrastructure scanning/reporting cycle	Monthly/Every two months/Quarterly
Policy compliance and/or Security Configuration Assessment ("**SCA**") scanning and reporting	Up to X*
Policy compliance and/or SCA Reporting Cycle	Monthly/Every two months/Quarterly
Number of websites	Up to X*
Website scanning/reporting cycle	Monthly/Every two months/Quarterly
*** Volumes are defined in Customer's Transaction Document for this Service.**	

Note: Refer to vendor documentation for information about maintenance for vendor's scanning platform.

2.2.2.1 Changes to Customer's Technical Environment

Changes to Customer's Technical Environment can result in changes to price. Customer and Secureworks will mutually agree if a change in Customer's Technical Environment will result in changes to price that is listed in the Transaction Document.

2.2.3 Configuration and Scanning Management

As Customer's infrastructure expands or decreases per business needs (e.g., devices being added or removed), corresponding changes will need to be made in the vulnerability scanning asset database. Secureworks will work with Customer to ensure information in the vulnerability scanning asset database is in alignment with Customer's infrastructure (i.e., ensure proper configuration). This enables technical owners to be accurately informed of the problems they need to manage.

To enable report generation and faster scan configuration, Secureworks will help ensure Customer's assets are distributed in asset groups and tags are assigned to assets according to customer environment details.

Authenticated scans provide visibility into Customer assets and identify with more precision the problems Customer should address. Secureworks will help ensure assignment of proper credentials with higher access rights to enable the scanning tool to connect to Customer's assets and execute authenticated scans.

2.2.3.1 Exclusions

Secureworks will manage exclusions for scans on an ongoing basis. Managing exclusions will prevent scanning of the excluded IP ranges and ports. Secureworks will work with Customer to identify the IP addresses (ranges) and ports to exclude from scans. Exclusions can be configured to expire, which enables the excluded IP ranges and ports to be included in future scans.

2.2.3.2 On-Demand (or Ad-Hoc) Scanning and Reporting

Secureworks will execute on-demand scanning and reporting based on Customer's requirements (targeted assets, scanning time-window, credentials to be used, and related information) that are submitted using the agreed-upon communication method. During Service Implementation, Customer and Secureworks will agree to a process for on-demand scans and reports.

An "On-demand Scan" is any request for a scan that Customer submits to Secureworks that is not part of the recurring scanning activity and involves scheduling or directly executing a scan against a defined target, and providing a report that is extracted from the scanning tool (without applying any vulnerability prioritization).

An "On-demand Report" is a request for a report from an On-demand Scan or other scans (such as scheduled scan for which Customer needs more information that Secureworks will add), which requires extracting the report from the scanning tool, collecting the additional information, and sending the report to Customer through agreed-upon communication method. On-demand reports do not include the standard reports that are automatically delivered to Customer from the scanning tool, without Secureworks involvement.

The total number of On-demand Scans and On-demand Reports that will be provided to Customer each month will be defined in Customer's Transaction Document. A request for a scan will automatically include a report (which counts as one request), or Customer can request only a report (which counts as one request). For example, if the total number is 15, and Customer requests one scan, this will count as one request, and a report will

automatically be included (the report does not count against the total of 15; Customer will have 14 remaining requests).

2.2.3.3 Standard and Custom Reporting

Secureworks will provide Customer with standard and custom reports containing vulnerability scan results, which include information about new, existing, and remediated vulnerabilities. The reports will enable Customer to view the state of an asset or group of assets (motivated by a business reason) at a single point in time, and track changes over time.

The standard reports provided are listed in Section 2.2.5, Reporting.

Custom reports are considered any reports that require data manipulation, correlation, and prioritization other than what is directly extracted from the tool. For any custom report requested, Secureworks will provide a report template to Customer, and Customer will review and return the template to Secureworks for creation of the custom report. If a custom report is deemed technically infeasible, then Secureworks will provide an alternative that is similar to meet Customer's report requirements, provided the report is within the scope of the Service.

The number of reports that will be provided to Customer is determined as follows:

- Number of Recurrent, Risk prioritized, Technical Reports (monthly or quarterly) will be less than or equal to the number of Customer Technical Representatives
- One Executive Report (provides information about current status of Customer's Vulnerability Management Program) will be delivered at the end of the recurrent scanning activity cycle (monthly or quarterly)
- Number of Custom reports available per month to Customer will be equal to the number of Customer Technical Representatives

2.2.4 Remediation Activities

The subsections below explain the vulnerability remediation coordination that Secureworks will provide.

2.2.4.1 Analysis of Scan Report Results

Secureworks will analyze scan results for accuracy, identify and solve configuration issues with the scans, and provide details about the reports based on information available from the scanning tool. This includes identifying and addressing scanning issues such as scans blocked by a firewall(s), issues with the scan duration, and vulnerability scanner load balancing.

2.2.4.2 Vulnerability Reprioritization

Secureworks will adjust remediation priority after correlating detected vulnerabilities with the following:

- Exploitability information
- Severity of the vulnerability
- Asset location (visibility through the Internet; if Customer provides information about network placement of assets)
- Value of the impacted assets (if Customer provides this information)

High impact vulnerabilities, and newly discovered vulnerabilities, will be accounted for and analyzed.

2.2.4.3 Remediation Guidance

The amount of vulnerabilities detected can be numerous and may require detailed analysis based on different environmental variables (e.g., Customer business domain, priorities, strategies, and resources). Therefore, Secureworks will provide infrastructure remediation suggestions, which includes the aforementioned analysis, and will provide to Customer

(particularly, Customer's technical owners of the data) the analysis, findings, and recommendations for remediation.

Secureworks will engage in periodic and on-demand Customer meetings regarding remediation and vulnerability management process improvement. Vulnerabilities and associated remediation, and solutions, will be discussed with the technical owners, based on available information. Technical owner-focused reports that reflect as accurately as possible the security status of scanned assets will be compiled and discussed.

2.2.4.4 Remediation Tracking

Secureworks will work with the Customer to track the remediation efforts of the patching teams. Given the situation, Secureworks Vulnerability Management team will escalate to the Customer's management any non-compliance from the Remediation Policy for corrective actions to be applied by it. Remediation tracking activity will not be applied for On-Demand scanning as, this activity, will only be tight to the recurrent scanning and reporting.

2.2.4.5 Exception Management and Documentation

Secureworks will work with Customer to manage the remediation exception process according to Customer's needs and requirements. Secureworks will provide guidance to Customer for addressing exceptions and ensure that exceptions are considered when scanning and remediation reports are compiled. An example of a potential exception would be an outdated production server using Windows XP that needs to be maintained to operate an old business-critical application. The application was internally developed and cannot be upgraded.

Documentation is important in maintaining process integrity and for support purposes in audits and compliance reviews. Secureworks will help Customer create and maintain documentation, including any updates or changes made to Customer's initial vulnerability management processes. Details about the exception process and its requirements are documented to be considered for later scans and reports.

2.2.5 Reporting

Listed in the table below are the reporting deliverables. The frequency for reporting ("**Per Reporting Period**" and "**Per Scanning Period**") is defined in Customer's Transaction Document. Some of the reporting deliverables are dependent on the BI Reporting Tool existing in Customer's environment (see Section 2.2.5.1, BI Reporting Tool).

Item	Deliverable	Description	Frequency
1	Percent of total systems monitored or scanned	Measures the completeness of Customer's vulnerability management scanning solution, whether it has awareness of all or some of its assets, and whether it is monitoring the assets	Per Scanning Period
2	Number of unique vulnerabilities	Measures the amount of variance of vulnerabilities that exist among systems	Per Reporting Period
3	Number of assets with vulnerabilities	Measures the amount of assets with vulnerabilities categorized by OS	Per Reporting Period
4	Open vulnerabilities categorized by severity	Overview of severity of the vulnerabilities within Customer's environment	Per Reporting Period

Item	Deliverable	Description	Frequency
5	Vulnerabilities categorized by functional group	Provides a view of Customer's environment from a functional perspective; data is categorized according to responsibility groups and technical owners will be able to track their progress over time, viewing resolved and overdue vulnerabilities while simultaneously reviewing the number of new vulnerabilities that appeared in Customer's environment	Per Reporting Period
6	Top offenders	Information about the most commonly seen vulnerabilities in Customer's environment, which can include assets that have the largest number of vulnerabilities; gaps in patching policies or exclusion processes may also be identified	Per Reporting Period
7	Website reports	Overview of the website that was scanned and the vulnerabilities detected	Per Reporting Period
8	Governance reporting with actions	Monthly Operations Review Quarterly Service Review	Monthly Quarterly
9	Vulnerability Management activity schedule	Develop and deliver a scanning schedule per Customer-defined scanning interval; schedule includes the scanning meetings, reporting, timeline, and occurrence	Per Scanning Period
10	Periodic delivery of scan reports	Delivery of agreed-upon reports to the Customer-designated recipients according to the agreed-upon reporting timeline and reporting format	Per Reporting Period
11	End of life assets	Measures the systems that are no longer supported by the vendor and should undergo an upgrade process	Per Reporting Period

2.2.5.1 BI Reporting Tool

Secureworks will provide Items 1 – 7 in the table above through the BI Reporting Tool (a Secureworks-developed reporting platform). This tool will be hosted in Customer's virtual environment for the duration of the Service. The initial deployment will occur during the Design and Build process.

Customer agrees to provide an internal hosting server or virtual machine (Linux OS) for deployment and administration of the BI Reporting Tool. Below are the specifications for the server or virtual machine.

- Minimum hardware requirements: Quad Core CPU 2.5GH, 500 GB Storage, 32 GB RAM
- Remote connectivity with administrative-level access for BI Reporting Tool installation and deployment through the agreed connectivity solution for the BI engineer
- Internet connectivity for installation of required libraries and dependencies (e.g., MariaDB, Apache, Python, Django)
- Internal connectivity to the server using HTTPS

- External connectivity from the server to the vulnerability scanning tool

Secureworks will be responsible for maintenance of the installed database solution, Web frontend, BI Reporting Tool core application and associated libraries. Customer is responsible to provide administration and hardening for the hosting server. This includes regular patching of the OS and supporting applications. See Section 2.4, Support for Private Virtual Environments, for more information.

2.2.5.2 Report Delivery

Secureworks will provide the above-listed deliverables to Customer POC(s) through email or Customer's secure file-sharing solution.

2.3 Service Delivery

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

2.3.1 Business Days and Support Hours

Business Days ***for the VMS Platinum Service*** are Monday-Friday, 10 a.m. – 7 p.m. Eastern European Time, excluding Romanian public holidays (https://publicholidays.ro/) that may vary each year. Customer support is available during the hours indicated in the table below.

Support Hours (Eastern European Time) Monday-Friday*	**Equivalent Support Hours (United States) Monday-Friday**			
	Pacific (San Francisco)	**Mountain** (Denver)	**Central** (Dallas)	**Eastern** (Atlanta)
10 a.m.–7 p.m.	Midnight–9:00 a.m.	1:00 a.m.–10:00 a.m.	2:00 a.m.–11:00 a.m.	3:00 a.m.–Noon

* Excluding Romanian Public Holidays

Secureworks personnel delivering the Service are located in a region observing Daylight Savings Time ("**DST**"). Time variances will exist for brief periods in the spring and fall when DST is transitioning, and for regions of the world not observing DST – e.g., Arizona in the United States ("**US**").

During time periods that are not within the above-listed support hours, on-demand support will be provided only if Customer needs help to suspend or cancel in-progress scans that are interfering with production systems. This on-demand support only applies to Customer's in-scope Environment to the extent that the scan is significantly impacting Customer's business operations and requires a response that cannot be delayed until support hours during the next Business Day. On-demand support will not be provided for routine tasks that are not emergencies and that can be performed during the above-listed support hours. Customer has up to 5 (five) times per month included in the Service to be used for on-demand support. All on-demand support situations will be further investigated during the above-listed support hours. On-demand support must be invoked through a Customer escalation process, which will be agreed to during service implementation.

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. These hours are applicable to activities such as maintenance-related activities (see Section 1.2.8, Maintenance) and Initial Implementation Scheduling (see Section 1.3, Initial Implementation Scheduling and Points of Contact).

2.3.2 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. Other components of the Service that are visible to Customer (such as reports and documentation) 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.

2.3.3 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.

Notes:

- The SOC provides Quick Start guides to Customer, which contains more detail about SOC-specific roles and responsibilities.
- If Customer purchases Qualys add-on modules, then the tasks listed below also indicate the responsibilities for Customer and Secureworks for the add-on modules. For example, if Customer purchases the SCA add-on module, then as indicated below in the "Scanning" section of the table, Secureworks will be responsible for the following task: "Validate success of policies and controls within Customer's environment."

Vulnerability Program Management – VMS Platinum				
Activity	**Task**	**Customer Mgmt.**	**Customer Tech. Team**	**Secureworks**
Service Preparation	Provide contact information for authorized contacts regarding Service-related activities	R, A	C	I
	Provide information for authorized users who need access to the vulnerability scanning tool	R, A	C	I
	Identify in-/scope assets (e.g., IPs, websites) applicable to the Service	A, I	R	C, I
	Provide Secureworks-assigned personnel with access to Customer environment	A	R	I
	Provide managerial and technical information from Customer's environment (e.g., existing Procedures,	R, A	C	C, I

Vulnerability Program Management – VMS Platinum				
Activity	**Task**	**Customer Mgmt.**	**Customer Tech. Team**	**Secureworks**
	Network Diagram)			
Service Implementation	Install physical, virtual, or agent-based vulnerability scanners		R, A	C, I
	Configuration and management of vulnerability scanners within the scanning tool		C, I	R, A
	Provide hardware and/or virtual resources for BI Reporting Tool	R, A		I
	Deploy BI Reporting Tool in Customer's environment	I	I	R, A
Scanning	Define scan schedules including frequency and approved times	A, I	C, I	R
	Implement scan schedules	I	I	R, A
	Configure logical asset groupings and scan schedules according to Customer's vulnerability scanning subscription	I	C, I	R, A
	Define report requirements	A	A	R
	Implement report requirements	I	I	R, A
	Create and manage authentication records for authenticated scanning	I	C, I	R, A
	Create and manage custom scanning configuration/option profiles	I	C, I	R, A
	Monitor scans to confirm completion or if an error occurred; restart scans if needed	I	I	R, A
	Identify any anomalies, errors, or network impacts regarding scan results and adjust scan (e.g., adjust option profile) as necessary	I	C, I	R, A
	Obtain and deliver to Customer the scan results	I	I	R, A
	Review each scan result (all vulnerability data) and report output (net	I	I	R, A

Vulnerability Program Management – VMS Platinum				
Activity	**Task**	**Customer Mgmt.**	**Customer Tech. Team**	**Secureworks**
	vulnerability data) and determine next steps			
	Integrate API data with custom (homegrown) and/or third-party tools	A	R	I
	Build/Import any policies (when technologically applicable) as necessary to measure compliance	A	C, I	R
	Customize control/plug-in values to match Customer-defined policy	I	C, I	R, A
	Provide to Secureworks blacklists and/or whitelists for website scans	I	R, A	C, I
	Identify needs for Customer-provided blacklists/whitelists for website scans and implement them in the scanning tool	I	C, I	R, A
	Validate success of policies and controls within Customer's environment	I	C, I	R, A
Remediation and Reporting	Develop and monitor KPIs to measure and track remediation efforts	C, I	I	R, A
	Review vulnerability reports to prioritize vulnerabilities and provide suggested remediation strategies to Customer	C, I	I	R, A
	Create custom reports (separate from standard, vendor-supplied reporting capabilities) if deemed technically feasible	C, I	C, I	R, A
	Provide remediation advice for specific vulnerabilities as applicable, based on scan results	I	I	R, A
	Review vulnerabilities within scanning tool	I	I	R, A
	Determine whether risk is accepted	A	R	I
	Implement vulnerability exception scanning tool and BI Reporting Tool as appropriate for each vulnerability	I	I	R, A

Vulnerability Program Management – VMS Platinum				
Activity	**Task**	**Customer Mgmt.**	**Customer Tech. Team**	**Secureworks**
	Remediate vulnerabilities	I	R, A	C
Support	Ensure Secureworks has current contact information for authorized contacts regarding Customer's account	R, A		I
	Provide support to Customer for issues relating to the Secureworks Client Portal (including mobile access)	I	I	R, A
General	Perform all Customer-side network changes (when needed)	A, I	R	C, I
	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

2.4 Support for Private Virtual Environments

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

Note: The Secureworks managed security services and associated SLAs are the same for both non-virtualized (physical) environments and virtual environments.

2.4.1 Customer Responsibilities

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

2.4.1.1 Provisioning and Maintenance

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

- Virtual switches
- Virtual network interfaces
- Virtual networks
- virtual machines

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

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

2.4.1.2 Virtual Machines

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

2.4.2 Secureworks Responsibilities

If Customer purchases Qualys licenses from Secureworks, then Secureworks is responsible for providing the VSA, providing support to Customer during provisioning of the VSA, and managing and monitoring the VSA that are operating on the Guest virtual machine(s). Customer must maintain a suitable environment in which to operate the Guest virtual machine(s) that is being used for the VSA. This includes using a Secureworks-supported Hypervisor version.

2.4.3 Shared Responsibilities

2.4.3.1 VSA Upgrades

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

2.4.3.2 VSA Backups

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

2.4.4 VSA Health, and Adding Capacity

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

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

Secureworks will perform availability monitoring of the VSA using periodic polling of each Device. If a failed or negative response is received through periodic polling, then an automatic alert is sent to Secureworks, which then generates a ticket. Secureworks will conduct troubleshooting and contact Customer as applicable to the Service.

Health monitoring is limited to VSAs and other Devices that are in scope for the Service. Secureworks does not perform health monitoring for Hypervisors or underlying hardware.

2.4.5 Out-of-Scope Services in a Virtual Environment

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

- Restoring the VM image backups
- Troubleshooting issues at the Hypervisor level
- Troubleshooting performance issues not directly related to the scanning tool such as hardware (e.g., a server that is hosting VMware with a scanning engine), Hypervisor, or Host-level issues
- Anything not specifically described herein as part of the standard offering for the Service

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 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 Transaction Document or Statement of Work ("**SOW**").

- Monitoring Security Events and alerting Customer about them
- Accessing the Scanning Portal directly (bypassing single sign-on from the Secureworks Client Portal)
- Supporting unsupported features, functionality, or modules

The Service does not include licenses to a vulnerability scanning subscription. Secureworks will perform the Service in this SD using Customer-provided vulnerability scanning subscription from Taegis VDR, Qualys, Tenable, or Rapid 7. If Customer does not have an existing license for a vulnerability scanning subscription, then Customer can purchase licenses for Qualys through Secureworks. See the Appendix for Qualys-specific information.

3 Service Fees and Related Information

Service Fees are based on the quantities for each of the deliverables (see list of deliverables in Section 1.1) as defined in Customer's Transaction Document. See Customer's MSA or CRA (as applicable), and Transaction Document or SOW (as applicable) for details, including the following:

- Billing and Invoicing

- Out-of-Pocket Expenses
- Services Term

3.1 Related Information

- The term of the Service shall commence on the Start of Services. The introductory call (through remote teleconference) will occur within 60 days after executed Transaction Document. If the introductory call 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 Services" 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 Services. The period of time from the Start of Services to the end of the calendar month will be added to and invoiced along with the second month's (the first full-service month) invoice.
- The Service shall terminate after the period specified in the Transaction Document.

4 Service Level Objectives ("SLOs")

The table below contains the SLOs that are applicable to the VMS Platinum Service. See Section 2.3.1, Business Days and Support Hours, for the definition of a ***Business Day as applicable to the VMS Platinum Service***.

Service	Delivery time	Observation/Limitation
On demand scan – Acknowledgement	2 Business Days	Included in the Service is a specified number of scans per month – see Section 1.1, Overview
On demand scan – Results delivery	2 Business Days	The timer starts after the scan finishes
Recurring scan – Results delivery	5 Business Days	The timer starts after the recurring scan finishes
Customer Meetings *****	Regular and on-demand	Included in the Service is a specified number of meetings per month***** – see Section 1.1, Overview
Scan configuration changes (e.g., changes to existing scanning option profiles, changes to existing report templates, new scanning profile creation, new report template creation)	3 Business Days	Included in the Service is a specified number of new profiles per month – see Section 1.1, Overview; profiles will not be created in the week when scanning is scheduled to run
Policy compliance changes	5 Business Days	Limited to the controls, policies, and standards already configured in the scanning tool
Implementation of exception	5 Business Days	
*** Note: Regular and on-demand customer meetings, including those for results and remediation discussions, are one hour in length.**		

SLO Name	Description	Minimum Performance Level	Calculation	Formula Variable A	Formula Variable B	Measurement Source
On-demand scan request acknowledgement	Secureworks will acknowledge Customer's request for an On-demand scan in accordance with Section 1.1 within two (2) Business Days	>=90%	Service Level performance = (A / B) x 100, expressed as a percentage	A = total number of times a request acknowledgement was created within two Business Days	B = total number of times an on-demand request was submitted	The Ticketing System of record
On-demand scan scheduling	In accordance with Section 1.1, Secureworks will schedule the scan within two (2) Business Days after the information provided by Customer is deemed whole and complete	>=90%	Service Level performance = (A / B) x 100, expressed as a percentage	A = total number of times an on-demand scan was scheduled within two Business Days	B = total number of times an on-demand scan was scheduled	The Ticketing System of record
On-demand scan results delivery	Secureworks will deliver the scan results after the scan has completed within two (2) Business Days	>=90%	Service Level performance = (A / B) x 100, expressed as a percentage	A = total number of times on-demand scan results were delivered within two Business Days	B = total number of times on-demand scan results were produced	The Ticketing System of record
Recurrent scan results delivery	Secureworks will deliver the scan results after the scans have completed within five (5) Business Days	>=90%	Service Level performance = (A / B) x 100, expressed as a percentage	A = total number of times on-demand scan results were delivered within two Business Days	B = total number of times on-demand scan results were produced	The Ticketing System of record

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:

- 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.

- 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 is dependent on Secureworks' ability to connect directly to Customer-Side Technology on Customer's network, and access the Service-specific tickets in the agreed-upon ticketing system.
- The SLOs shall not apply in the event that Customer-Side Technology is unreachable for reasons that are not within the direct control of Secureworks, such as network connectivity issues, authentication issues, configuration issues, or public cloud unavailability.

5 Appendix

If Customer purchases Qualys licenses from Secureworks, then the information in this Appendix is applicable to the Service. Additional steps must be completed during Service Implementation, and Customer is provided with access to service-enabling technology as described below.

Customer acknowledges and agrees that (i) Customer's purchase and use of the Qualys license is governed by the terms and conditions set forth at https://www.secureworks.com/third-party-terms/qualys, and (ii) Secureworks makes no representations or warranties of any kind with respect to the Qualys license and shall not be responsible for any damages associated with the Qualys license.

5.1 Qualys Scanning Subscription Implementation

Secureworks will execute the steps described below as part of implementation for Qualys subscriptions/licenses only. Secureworks team members will work in parallel to implement both VM Program Development and the Qualys scanning subscription.

See the Secureworks VMS Addendum – Qualys Add-on Modules document for information about the Secureworks-supported Qualys add-on modules.

- **Organize:** Execute provisioning steps, which consist of the initial actions that are completed in advance of implementing the Service for Customer, such as configuring the scanning subscription and enabling Qualys Scanning Portal and Secureworks Client Portal access (including confirming Customer's ability to access both portals)
    - Secureworks will work jointly with Customer to validate accuracy of the information used to create the original Transaction Document 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 Transaction Document may be required, which may include changes to scope and fees, and (ii) without such an amended or additional Transaction Document, Secureworks may only be able to provide the subscription as scoped, defined, and charged per the original Transaction Document. In some cases, an amended or additional Transaction Document may be required to provide the subscription in the original Transaction Document. For example, an additional CTA may be required at a location that was not originally determined to be in scope.

- **Prepare:** Provide scanners to Customer for installation; Customer provides information necessary to execute implementation for Vulnerability Management Scanning ("**VMS**")
  - Installation consists of configuring the subscription, sending physical scanner(s) to Customer through ground shipping method, and testing connectivity of the scanner(s) (***Note:*** Installation and completion of minimal configuration by Customer for scanner is required.)
- **Execute:** Customer completes configuration of scanners (if applicable) and Customer provides details of Hosts that comprise the VMS subscription; Secureworks will configure the VMS subscription based on this information and confirm scanner connectivity
- **Rationalize:** Confirm Customer's ability to access Qualys subscription using single sign-on through the Secureworks Client Portal
- **Accept:** Validate successful deployment of the Qualys scanning subscription implementation

5.1.1 Provisioning a Virtual Scanner ("vScanner") into a Virtual Environment

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

Secureworks will provide Customer with an image to install on the Hypervisor in Customer's Public Cloud or Private Virtual Environment. The image is used to create the vScanner on a Guest Virtual Machine. Customer will access the Qualys Scanning Portal (through the Secureworks Client Portal) and complete steps to obtain the image for the vScanner. Depending on Customer's environment, the specific steps for installing and provisioning the vScanner may vary, and Secureworks will provide applicable information to Customer.

When provisioning the vScanner into a virtual environment, Customer is responsible for creating and supporting the underlying Guest Virtual Machine. This includes all management and maintenance of the Guest Virtual Machine (i.e., the Host), Hypervisor, and related hardware.

When provisioning the vScanner, Customer is responsible for network configuration (including assigning an IP address, net mask, gateway) to the vScanner. See Section 2.4, Support for Private Virtual Environments, for more information about virtual environments including additional Customer responsibilities.

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

5.2 Service-Enabling Technology

If Customer purchases Qualys licenses from Secureworks, then Customer will be supported in deploying configuration and help testing of new features and functionalities during accepted Proof-of-Concepts, based on the limits of the Service Descriptions and Transaction Documents limitations with the express approval of Customer representatives.

6 Glossary

Term	Description
Due Diligence	Validating the accuracy of information used to create the Customer's original Service Order against the actual environment in which Services will be performed.
Identified Changes	Differences (e.g., Device quantity, make, model, software package, or software version) that are discovered while conducting due diligence for the Service.
In-Band	Activity within a defined telecommunications frequency band.
Private Virtual Environment	Customer’s on-premises virtual infrastructure.
Public Cloud Environment	Third-party virtual infrastructure that hosts the Customer’s network and security devices.
Qualys Scanning Portal ("**Scanning Portal**")	The portal provided in the Qualys solution that provides Customer with reporting capabilities.
Definitions for Virtual Environments	
Guest	Separate and independent instance of operating system and application software that operates on a Host.
Host	Virtual Machine Host server that provides the physical computing resources, such as processing power, memory, disk, and network I/O.
Hypervisor	Virtual Machine monitor that isolates each Guest, enabling multiple Guests to reside and operate on the Host simultaneously.
Virtual Contexts	A form of virtualization where one physical firewall is divided into two (2) or more virtual firewalls.
Virtual Machine	A logical instance of the physical Host that houses the operating system of the Guest.
Virtual Security Appliance (“**VSA**”)	Software implementation of a security device—e.g., a log retention appliance, scanner appliance (VMS), intrusion detection system—that executes programs in the same manner as a physical machine.