

# Monitoring Service Description and Service Level Agreements

This Service Description and Service Level Agreement is provided for the customer ("you" or "Customer") and the Dell entity identified in the Customer's Service Order for the purchase of this Service (defined below). This Service is provided in connection with the Customer's separate signed master services agreement or security services schedule that explicitly authorizes the sale of managed security services. In the absence of either a master services agreement or security services schedule, this service is provided in connection with the Dell SecureWorks Master Services Agreement, available at <a href="http://Dell.com/SecurityTerms">http://Dell.com/SecurityTerms</a> and incorporated by reference in its entirety herein.

#### Service Overview

The Dell SecureWorks® Security Monitoring service provides real-time, security event analysis and response across your security and critical infrastructure 24 hours a day, 7 days a week, 365 days a year.

## **Detailed Description**

#### **Features**

Feature	Description	
Dell SecureWorks Customer Portal	Provides ticketing workflow management for incident management and other Security Operations Center ("SOC") interaction. Also provides real-time visibility and reporting of your security events and associated incidents.	
Health and Performance Monitoring	Health monitoring using event trending technology to ensure that the SOC is receiving events from your monitored systems 24 hours a day, days a week, and 365 days a week.	
Security Event Monitoring	Automated monitoring of logs to identify and respond to security threats 24 hours a day, 7 days a week, and 365 days a week.	
SOC Access	Non-metered access to our security analysis staff across our Security Operations Centers via the ticketing system, email, and phone.	

#### Service Activation

Dell SecureWorks Security Monitoring Service Activation consists of three main phases: Information Gathering, Counter Threat Appliance ("CTA") Deployment, and Service Provisioning and Installation.

## Information Gathering

When Dell SecureWorks receives the Services Order, Dell SecureWorks provides Customer with a Service Initiation Form ("SIF") to be completed. When Customer has returned the completed SIF, Dell SecureWorks schedules a conference call to review the completed document and other relevant information.



#### CTA Deployment

Using data gathered during the Information Gathering phase, Dell SecureWorks determines the appropriate CTA deployment location(s) within Customer's environment. If changes to Customer's existing network architecture are required for Service implementation, Dell SecureWorks communicates these changes to Customer. For Services requiring the use of the CTA, Customer is responsible for ensuring that the implementation site complies with Dell SecureWorks physical/environmental requirements.

Service interruptions or failure to achieve the SLAs will not be subject to penalty in the event of non-compliance with the above CTA deployment guidelines.

Dell SecureWorks reserves the right, in its reasonable discretion, to utilize one or more CTAs deployed in a Dell SecureWorks data center to communicate with devices Dell SecureWorks is monitoring, in lieu of CTA(s) deployed in Customer's network. In such case, none of the provisions around the CTA apply.

#### Service Provisioning and Installation

The Service Provisioning and Installation phase begins upon the completion of the Information Gathering phase described above.

Service Provisioning and Installation is performed in the following manner:

- New devices to be deployed are shipped directly to Dell SecureWorks for configuration and subsequent shipment to Customer location.
- Existing equipment in use is provisioned remotely with on-site support from Customer.
- Dell SecureWorks provides telephone support to Customer contact at the implementation site during installation of all Customer premises equipment.
- Once Customer premise equipment is in place, Dell SecureWorks accesses the device(s) remotely and performs the remaining configuration and service activation tasks which may require device downtime.

Dell SecureWorks schedules service provisioning and installation in accordance with change management procedures communicated by Customer during the Information Gathering phase. Standard installations are performed during the hours of 9 am and 5 pm EST, Monday through Friday, and may be performed at other times for an additional fee.

## Service Components

Dell SecureWorks' Counter Threat Platform<sup>TM</sup> ("CTP") provides the foundation for delivery of our Managed Security Services. This Dell SecureWorks-developed technology facilitates device management, health monitoring, security analysis, and customer reporting.

## Health Monitoring

The Counter Threat Platform provides passive health checks on monitored devices. Passive checks are performed using event flow trending technology to detect degradation or loss of log collection from managed and monitored devices. Any checks that identify system issues are escalated to the Health Team in the SOCs for analysis and escalation, if needed, to help ensure that infrastructure is operating at peak performance. Device health information and ticketing workflow is displayed in the Portal for customer consumption.



#### Security Analysis

The Counter Threat Platform can aggregate and correlate security events from virtually<sup>1</sup> any device including Firewalls, IDS/IPS sensors, and servers. This industry-leading Dell SecureWorks-developed technology processes log and alert information to escalate security events to the customer. Customers can view security events and perform incident workflow through the Customer portal.

#### Customer Portal

Dell SecureWorks' industry-leading Customer portal provides real-time security and service delivery visibility across all the services delivered to your organization. Using the portal, customers can run security and compliance reports, view high level graphical information including trending and comparative charts, and interact with the Dell SecureWorks SOC through tickets 24 hours a day, 7 days a week, and 365 days a year.

#### **Customer Requirements**

Customer agrees to perform the obligations and acknowledges and agrees that Dell SecureWorks' ability to perform its obligations and its liability under the SLAs below are interdependent on Customer's compliance with the following:

#### Monitored Device Health

Customer is responsible for appropriately maintaining the devices being monitored. In the event of a device failure or misconfiguration, Customer will be responsible for the actions necessary to bring the device back online. Additionally, Customer should communicate any network or system changes that could impact service delivery to the SOC via a ticket in the Dell SecureWorks Customer Portal. SLAs will not apply to devices that are experiencing health issues.

## Connectivity

Customer will provide access to Customer-premises and relevant system(s) and management console(s) necessary for Dell SecureWorks to monitor the contracted infrastructure. Additionally, Customer should communicate any network or system changes that could impact service delivery to the SOC via a ticket in the Dell SecureWorks Customer Portal. SLAs will not apply to devices that are experiencing customer-caused connectivity issues.

#### Export

Customer acknowledges that the Products, Software and Services provided under this agreement, which may include technology and encryption, are subject to the customs and export control laws and regulations of the United States, and may be rendered or performed either in the U.S., in countries outside the U.S., or outside of the borders of the country in which you or your system is located, and may also be subject to the customs and export laws and regulations of the country in which the Products, Software or Services are rendered or received. Customer agrees to abide by those laws and regulations.

Classification: //Dell SecureWorks/Confidential - Limited External Distribution:

<sup>&</sup>lt;sup>1</sup> Alerts and logs must be sent via syslog or snmp standard protocols or the following APIs: IBM SiteProtector Database, McAfee ePO Database, Sourcefire eStreamer, Cisco SDEE and OPSEC LEA



## Service Agreements Level (SLAs)

#### Service Level Agreements Matrix

SLA	Definition	SLA Credit
Standard Help Desk Requests	Standard help desk requests (applies to all non-change and non-incident tickets) submitted via the Dell SecureWorks Customer Portal or via telephone will be subject to "acknowledgement" (either through the help desk ticketing system, email or telephonically) within one (1) hour from the time stamp on the Help Desk ticket created by Dell SecureWorks.  An acknowledgement to Help Desk requests classified as "Emergency" on the Help Desk ticket and verified by the SOC as "Urgent" will be sent (either through the help desk ticketing system, email, or by telephone) within fifteen (15) minutes from the time stamp on the Help Desk ticket created by Dell SecureWorks.	1/30 <sup>th</sup> of monthly fee for Service
Security Monitoring	Customer shall receive a response (according to the escalation procedures defined in the Customer Portal or in the manner preselected in writing by Customer, either through the help desk ticketing system, email, or by telephone) to security incidents within fifteen (15) minutes of the determination by Dell SecureWorks that given malicious activity constitutes a security incident. This is measured by the difference between the time stamp on the incident ticket created by Dell SecureWorks SOC personnel or technology and the time stamp of the correspondence documenting the initial escalation.	1/30 <sup>th</sup> of monthly fee for Service for the affected device
	A "security incident" is defined as an incident ticket that comprises an event (log) or group of events (logs) that is deemed high severity by the SOC in accordance with Dell SecureWorks' Event Handling Process (see Exhibit A). The most up-to-date version can always be found in the Real-Time Events section of the Customer portal).	
	Automatically created incident tickets (via correlation technology) and event(s) or log(s) deemed low severity will not be escalated, but will be available for reporting through the Customer portal.	

#### Additional Service Rules, Regulations, and Conditions

- a. Dell SecureWorks Security Monitoring service provides expert security analysis and response to the customer. However, deployment of Dell SecureWorks' managed services in a Customer network does not achieve the impossible goal of risk elimination, and therefore Dell SecureWorks makes no guarantee that intrusions, compromises, or any other unauthorized activity will not occur on a Customer network.
- b. Dell SecureWorks may schedule maintenance outages for Dell SecureWorks owned equipment/servers which are being utilized to perform the services with 24-hours' notice to designated Customer contacts.
- c. The Service Levels set forth herein are subject to the following terms, conditions, and limitations:

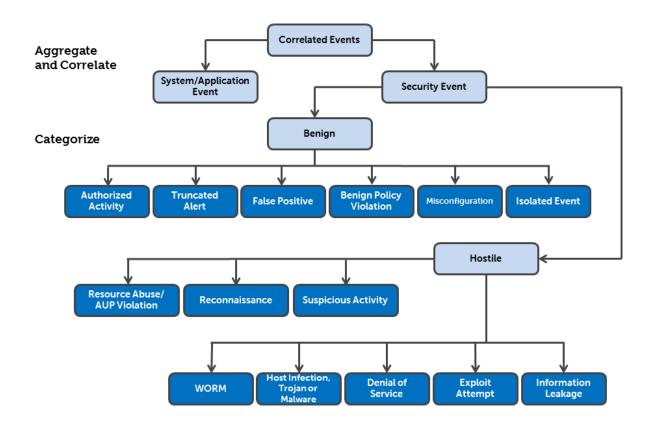


- i. The Service Levels shall not apply during scheduled maintenance outages and therefore are not eligible for any Service Level credit.
- ii. The Service Levels shall not apply in the event of any Customer-caused service outage that prohibits or otherwise limits Dell SecureWorks from providing the Service, delivering the Service Levels or managed service descriptions, including, but not limited to, Customer's misconduct, negligence, inaccurate or incomplete information, modifications made to the Services, or any unauthorized modifications made to any managed hardware or software devices by the Customer, its employees, agents, or third parties acting on behalf of Customer.
- iii. Furthermore, the Service Level's shall not apply to the extent Customer does not fulfill and comply with its obligations and interdependencies set forth within this SLA. The obligations of Dell SecureWorks to comply with the Service Levels with respect to any incident response or help desk request are also interdependent on Dell SecureWorks' ability to connect directly to the Customer devices on the customer network through an authenticated server in the Dell SecureWorks Secure Operations Center.
- d. Dell SecureWorks will troubleshoot and, if necessary, replace any iDevices in accordance Exhibit B Dell SecureWorks Maintenance Program Terms and Conditions.
- e. Customer will receive credit for any failure to meet the Service Level outlined above within thirty (30) days of notification by Customer to Dell SecureWorks of such failure. In order for Customer to receive a Service Level credit, the notification of the Service Level failure must be submitted to Dell SecureWorks within thirty (30) days of such failure. Dell SecureWorks will research the request and respond to Customer within thirty (30) days from the date of the request. The total amount credited to a Customer in connection with any of the above Service Levels in any calendar month will not exceed the monthly Service fees paid by Customer for such Service. Except as otherwise expressly provided hereunder or in the Agreement, the foregoing Service credit(s) shall be Customer's exclusive remedy for failure to meet or exceed the foregoing Service Levels.



# Exhibit A – Dell SecureWorks' Event Handling Process

## **Event Handling Process**





# Exhibit B – Dell SecureWorks Maintenance Program Terms and Conditions

- Dell SecureWorks agrees, subject to the terms and conditions of your separate master service
  agreement or security services schedule (and as further set forth below), to replace Dell
  SecureWorks iDevices that are not properly functioning adequately due to ordinary wear and
  tear, malfunctions, inadequate available memory, or obsolescence. Replacement devices may
  be new or refurbished.
- iDevices subject to this Program may include the Dell SecureWorks' Counter Threat Appliance (CTA), iSensor, LogVault appliance, Inspector, SDA, SYSLOG Aggregator, log collection devices, and/or SNORT IDS device.
- The charges for the Program only cover replacement of Dell SecureWorks iDevices. Any performance, damage, repair and/or other warranty issues, or claims with respect to non-Dell SecureWorks-branded iDevices must be addressed with the applicable OEM manufacturer.
- Dell SecureWorks' obligation to comply with the foregoing is conditioned upon, and subject
  to, the assistance and availability of Customer's onsite personnel for assistance in the: (x)
  diagnosis and troubleshooting of problems with existing iDevices and (y) replacement and
  installation of any new iDevice all in compliance with your master service agreement or
  services schedule.
- Furthermore, Dell SecureWorks will not replace Dell SecureWorks iDevices returned by Customer that are no longer performing on account of unauthorized use, physical damage, or misuse or abuse of the products, as determined by Dell SecureWorks in its sole discretion, including, but not limited to, any of the following circumstances:
  - 1. Damage due to lightning or other climate problems (including, but not limited to, exposure to excessive light, heat, flooding, and the like)
  - 2. Opening of iDevices by any person other Dell SecureWorks authorized personnel
  - 3. Unauthorized loading or modification of software on or other reprogramming of the iDevice
  - 4. Unauthorized linking of the iDevice with other Customer equipment or systems
  - 5. Cracks in iDevices, dents to chassis or apparatus, or other damage caused by dropping of iDevice or other mishandling, misuse, or abuse
  - 6. Presence of liquids (or residue there from) or the excessive presence of other extraneous materials inside the iDevice (including, but not limited to, dust, hair, dirt, or grime)
  - 7. Inability to mount the iDevice
  - 8. Improper powering down of the iDevice
- Dell SecureWorks shall bill Customer, and Customer shall be liable, for iDevices: (i) damaged due to misuse or abuse, or (ii) no longer performing adequately due to unauthorized use, physical damage, misuse, or abuse of the iDevices.
- Upon termination of service, Customer is responsible for returning any iDevices (except those purchased by Customer) to Dell SecureWorks within 30 days