Service Description: Advanced Services – Fixed Price

Cisco Security Stealthwatch SIEM Integration Service (ASF-CORE-SWSIEM)

This document describes the fixed price Cisco Security Stealthwatch SIEM Integration Service.

Related Documents: This document should be read in conjunction with the following documents also posted at www.cisco.com/go/servicedescriptions/ : (1) Glossary of Terms; (2) List of Services Not Covered. All capitalized terms in this description have the meaning ascribed to them in the Glossary of Terms.

Direct Sale from Cisco. If you have purchased these Services directly from Cisco for your own internal use, this document is incorporated into your Master Services Agreement, Advanced Services Agreement, or other services agreement covering the purchase of Advanced Services-based services with Cisco ("Master Agreement"). If no such Master Agreement exists, then this Service Description will be governed by the terms and conditions set forth in the Terms & Conditions Agreement posted at http://www.cisco.com/web/about/doing_business/legal/terms_conditions.html. If you have purchased these Services directly from Cisco for resale purposes, this document is incorporated into your System Integrator Agreement or other services agreement covering the resale of Advanced Services ("Master Resale Agreement"). If the Master Resale Agreement does not contain the terms for the Purchase and Resale of Cisco Advanced Services or equivalent terms and conditions, then this Service Description will be governed by the terms and conditions of the Master Resale Agreement and those terms and conditions set forth in the SOW Resale Terms & Conditions Agreement posted at: http://www.cisco.com/web/about/doing_business/legal/terms_conditions.html. For purposes of the SOW Resale Terms and Conditions this Service Description shall be deemed as a Statement of Work ("SOW"). In the event of a conflict between this Service Description and the Master Agreement or equivalent services exhibit or agreement, this Service Description shall govern.

Sale via Cisco Authorized Reseller. If you have purchased these Services through a Cisco Authorized Reseller, this document is for description purposes only; is not a contract between you and Cisco. The contract, if any, governing the provision of this Service will be the one between you and your Cisco Authorized Reseller. Your Cisco Authorized Reseller should provide this document to you, or you can obtain a copy of this and other Cisco service descriptions at www.cisco.com/go/servicedescriptions/.

To purchase the Services, Customer must maintain an active support and maintenance agreement covering the Stealthwatch offerings that are the subject of the Services.

Security Stealthwatch SIEM Integration Service

Service Summary

The Cisco Security Stealthwatch SIEM Integration Service is intended to enable Customer's Security Operations Center (SOC) team to pivot directly from the SIEM console to Stealthwatch Security System to request a set of flow data from the Stealthwatch System to classify potential threats and to take appropriate action.

The service includes:

- Installation of Cisco's proprietary software appliance (Professional Services Integration Appliance or PSIA) that receives SIEM requests for Stealthwatch "TOP" reports for specific IP addresses and time frames.
- Completion of the SIEM Integration for Stealthwatch System over a period of up to 2 contiguous business weeks (10 days, Mon-Fri or Sun-Thur) during Standard Business Hours excluding Cisco holidays, locally recognized country holidays, vacations and training days.
- Document and train for the operation and configuration of Cisco's proprietary software appliance.

Stealthwatch installation, configuration, and tuning are not included as a part of this service, nor is any script writing or code development on non-Cisco devices.

Location of Services

Services are delivered both remotely or on-site to Customer as agreed upon providing up to a ten (10) day engagement. Where Customer desires on-site delivery, travel will be limited to no more than one (1) visit of up to four (4) days on-site at a single Customer location during Standard Business Hours excluding Cisco holidays, locally recognized country holidays, vacations and training days. Where on-site travel is agreed upon, travel must be arranged at least two (2) weeks in advance.

Delivery of Service

Cisco Responsibilities

Service Activities may include the following:

- Installation of Cisco's proprietary software appliance on a Linux based virtual machine or hardware appliance.
- Configure logic to fetch TOP reports based on SIEM requests. Types of aggregated data may be:
  - TOP ports
  - TOP peers
  - TOP conversations
  - TOP services
- Ensure alarm information is sent to the SIEM
- Document the use and configuration of the Cisco proprietary software appliance.
- Service is limited to completion of activities described above or performance of the Services over a period up to 2 contiguous business weeks (10 days, Mon-Fri or Sun-Thur), whichever concludes earlier.

Customer Responsibilities

- Designate a person to whom all Cisco communications may be addressed and who has the authority to act on all aspects of the service. Customer shall designate a backup when the Customer contact is not available, who has the authority to act on all aspects of the service in the absence of the primary contact.
- Customer will install the PSIA which will be provided to them as VMWare OVA.
- Customer provides server platform with the minimum requirements provided in the table below:

	CPU Number	CPU Specs	Memory	HDD	NIC
Virtual Machine	2 socket(s) with 2 cores each	2.9G>	8G DDR3>	100G	Single Gig NIC
Physical Machine	1 socket(s) with 2 cores each	2.4G>	8G DDR3>	100G	Single Gig NIC

- The Stealthwatch System is installed, operational, and receiving flows.
- Provides knowledgeable staff to assist Cisco with any scripting necessary for external devices. This includes an engineer who has full knowledge of the SIEM being used, if applicable. If external professional services engineers are required, Customer provides access to work directly with the SIEMS PS engineer to complete the integration with the SIEM.

General Customer Responsibilities

- All information (such as but not limited to: designs, topologies, requirements) provided by Customer is assumed to be up-to-date and valid for the Customer's current environment. Cisco Services are based upon information provided to Cisco by Customer at the time of the Services.
- Customer acknowledges that the completion of Services is dependent upon Customer meeting its responsibilities as indicated herein.
- Customer is responsible for obtaining all applicable software licenses.
- Customer will identify Customer's personnel and define their roles in the participation of the Services. Such personnel may include but is not limited to: architecture design and planning engineers, and network engineers, and project managers.
- Customer will ensure Customer's personnel are available to participate during the course of the Services to provide information and to participate in scheduled information gathering sessions, interviews, meetings and conference calls.
- Customer will provide forty-eight (48) hour notice in the event of cancellation of a pre-scheduled meeting.
- Customer expressly understands and agrees that support services provided by Cisco comprise technical advice, assistance and guidance only.
- Customer expressly understands and agrees that the Services shall take place and complete within ninety (90) calendar days from issuing a Purchase Order to Cisco for the Services herein.
- Customer will provide Cisco with access to Customer's site and facilities as required to enable Cisco to complete the services agreed upon schedule, including where applicable, computers, telecom equipment, facilities, workspace and telephone for Cisco's use during the project.
- Customer retains all responsibility for the security of its network. Cisco shall have no responsibility for, or liability as a result of, any breach in security of Customer's network.
- Customer will provide Cisco with secure VPN remote access for online services activity.
- Customer will provide Cisco employees and/or subcontractors with proper security clearances and/or escorts as required to access the Customer site.
- Customer will provide Cisco with its workplace policies, conditions and environment in effect at the Customer site.

Invoicing and Completion

Invoicing

Services will be invoiced upon completion of the Services.

Completion of Services

Cisco will provide written notification upon completion of the Services to Customer. The Customer shall within five (5) Business Days of receipt of such notification provide written acknowledgement of Cisco's completion of the Services. Customer's failure to acknowledge completion of the Services or to provide reasons for rejection of the Services within the five (5) Business Day period signifies Customer's acceptance of completion of the Services in accordance with this Service Description.